Draft ETSI GS QKD 0010 V0.0.1 (2017-12)

Quantum Key Distribution (QKD); Implementation security: protection against Trojan horse attacks in one-way QKD systems

Disclaimer

This DRAFT is a working document of ETSI ISG QKD. It is provided for information only and is still under development within ETSI ISG QKD. DRAFTS may be updated, deleted, replaced, or obsoleted by other documents at any time.

ETSI and its Members accept no liability for any further use / implementation of the present DRAFT.

Do not use as reference material.

Do not cite this document other than as "work in progress".

Approved and PUBLISHED deliverables shall be obtained via the ETSI Standards search page at: http://www.etsi.org/standards-search

This draft is being developed by the Quantum Key Distribution (QKD) ETSI Industry Specification Group (ISG) but it does not yet represent the considered views of all members who participated in this ISG.

It does not necessarily represent the views of the entire ETSI membership.

Reference

DGS/QKD-0010_ISTrojan

Keywords

quantum cryptography,
Quantum Key Distribution

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-préfecture de Grasse (06) N° 7803/88

Important notice

If an approved Group Specification results from this draft it will be made available for download from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group Quantum Key Distribution (QKD).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document describes protection for QKD systems against Trojan horse attacks launched against the time-varying phase, polarisation or intensity modulators that encode or decode bit values and / or basis values and / or the intensities of signal decoy and vacuum states on the quantum channel. It discusses the design, measurement and operation of one-way single-photon or weak-laser-pulse Mach-Zehnder QKD systems with decoy states where a fibre optic link is used as the quantum channel between the parties.

The attacks considered involve attempts by an adversary to obtain information about the state of an active time-varying phase, polarisation or intensity modulator that resides within the security boundary of a QKD transmitter or receiver module and where information is carried to the adversary by optical radiation exiting the security boundary of the module through a fibre optic quantum channel. The optical radiation carrying this information will have been previously inserted into the same module by the adversary via the same fibre optic quantum channel.

Modules where the quantum channel is multiplexed with other quantum or classical signals within the security boundary of the system are not within the scope of the present specification but in many cases implementers may consider an internal security boundary in order to apply this specification.

The present document attempts to describe current best practice based on the currently available knowledge.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI GS QKD 0011 v1.1.1: "Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems".

[2] EN 60793-1-40:2003: "Optical fibres — Part 1–40: Measurement method and test procedures — Attenuation".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1]

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

additional optical isolation: optical isolation to be inserted as additional protection that was not included during measurements of a module to determine an upper bound on its reflectivity

measured internal reflectivity: the reflectivity from all interfaces and components that could potentially contain any information about active optical components in the quantum channel within the security boundary as measured without the additional optical isolation in place

quantum channel: single-mode fibre optical path between the QKD sender and receiver units through which the optical pulses used for key transfer pass from the sender to the receiver

quantum port: single-mode optical fibre port on the case of the transmitter / receiver unit that carries the quantum signals

relevant reflectivity: the reflectivity from all interfaces and components that could potentially contain any information about active optical components in the quantum channel within the security boundary of the module including the additional optical isolation

relevant wavelengths: wavelengths within the range admitted by the spectral filter that must form part of the protection on the quantum channel between the polarising beam splitter that combines (splits) the two arms of the interferometer into (out of) the single fibre connected to the quantum port on the transmitter (receiver) and the quantum port itself

security boundary: the boundary of a module within which an adversary is assumed to have no physical access

NOTE: The adversary may communicate with components within the security boundary only via the permitted quantum and classical channels but direct physical access is prevented.

Trojan horse attack: attack on a QKD system where optical radiation is inserted by an adversary into apparatus under the control of a sender and / or receiver in order to measure information about the state of active optical components within quantum channel inside the apparatus

EXAMPLE: Optical pulses might be inserted into the quantum port of phase-modulated QKD transmitter module and photons introduced by the adversary that are reflected from an optical interface beyond the phase-modulator may be measured by the adversary to gain information about the basis used to encode bit values enabling the adversary to know how to measure the bit values from the signal photons or in some systems the phase of reflected photons might directly contain information about the bit values sent.

NOTE: The optical radiation enters said apparatus via the normal quantum channel for the entry / exit of photons used for key exchange. Information is leaked back to the adversary via a portion of the previously inserted optical radiation exiting the apparatus via the normal quantum channel.

NOTE: The adversary may combine the information leaked in this manner with information obtained from that intentionally encoded on either the quantum or classical channels by said apparatus. Any attempt by the adversary to combine information from Trojan horse attack with an attempt to exploit any other side-band or vulnerability or to attempt to interfere with the QKD module apparatus in any other manner would be considered a joint attack and not a pure Trojan horse attack.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

$c_{cal}(t)$	Number of detector events in single step of efficiency calibration OTDR scan with delay t
C_{cal}	Total number of detector events with sum range of efficiency calibration OTDR scan
$c_{DUT}(t)$	Number of detector events in single step of OTDR scan on a DUT with delay t
C_{DUT}	Total number of detector events contributing to the relevant reflectivity in OTDR scan on a DUT

D Average number of detection events per integration period in the absence of illumination on the detector

δ Time step in gate delay scan

f Finish index for summing data from the OTDR scan

μ_{in} Upper bound to the mean photon number of Trojan horse signals that could be injected into the transmitter per state prepared by the transmitter before it is rendered non-functional

μ_{out} Upper bound to the mean photon number of reflected Trojan horse signals exiting the transmitter per state prepared by the transmitter before it is rendered non-functional

r_{mi} Measured internal reflectivity

r_{rel} Relevant reflectivity

s Start index for summing data from the OTDR scan on a DUT

s' Start index for summing data from the efficiency calibration OTDR scan

T Time period of the laser source

T_{12} Transmission of the fibre optic direction coupler from port 1 to port 2

T_{AOI} Transmission of the additional optical isolation that was not present in measurements performed to determine the measured internal reflectivity

T_{SA} Transmission corresponding to the difference between the calibrated optical attenuator settings for the efficiency calibration OTDR scan (see clause 6.5.2) and the final OTDR scan $T_{\text{SA}} = T_{\text{SA\_high}} / T_{\text{SA\_low}}$

$T_{\text{SA\_high}}$ Transmission of the calibrated optical attenuator in its high-attenuation setting as used for efficiency calibration OTDR scans (see clause 6.5.2)

$T_{\text{SA\_low}}$ Transmission of the calibrated optical attenuator in its high-attenuation setting as used for OTDR scans on the DUT (see clause 6.5.9)

T_{vA} Transmission of the additional attenuation added by an optional variable attenuator inside a transmitter module during QKD operation over the attenuation of this component during reflectivity measurements

NOTE: Where a variable attenuator is not provided or adjusted within the transmitter unit to allow the measurement of lower internal reflectivities T_{vA} shall be taken to be unity.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

DUT	Device Under Test
FWHM	Full Width at Half Maximum
GSPD	Gated Single Photon Detector
OTDR	Optical Time Domain Reflectometry

4 Approach to Trojan horse attack protection

The approach adopted in this specification to protecting QKD modules against Trojan horse attacks starts by determining an upper bound to the optical power that could usefully be inserted into the module by an adversary. This may be based on the damage thresholds of at least one component of the module, such as optical fibre within the security boundary of the module, for example. Optical isolation can be inserted at the entrance to the module to protect the active phase, polarisation or intensity modulator(s) from Trojan horse attacks. Such optical isolation limits relevant reflectivity of the module and the amount of information that the adversary can obtain using such an attack. Privacy amplification is then used to remove any such information obtained by the adversary.

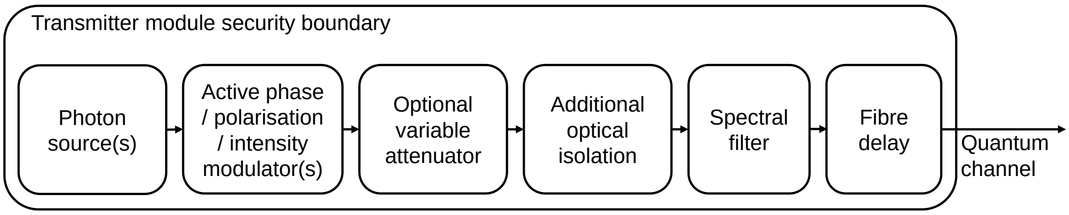
Transmitter module security boundary
Photon source(s)
Active phase / polarisation / intensity modulator(s)
Optional variable attenuator
Additional optical isolation
Spectral filter
Fibre delay
Quantum channel

Figure 1: Overview of transmitter protection

Attenuators and optical isolators may be inserted to protect transmitter modules. Receiver modules operating some protocols may in appropriate implementations obtain protection by introducing a sufficient length of optical fibre, to act as a delay line with the receiver module, without needing to insert additional optical isolation.

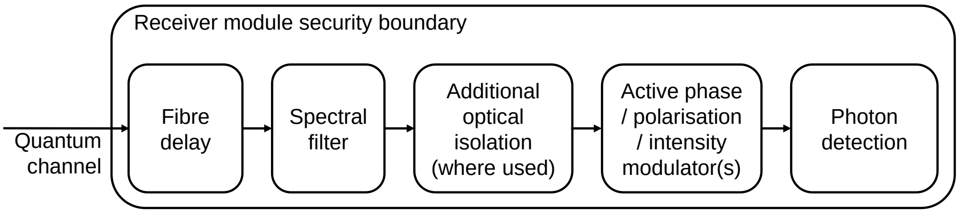
Receiver module security boundary
Quantum channel
Fibre delay
Spectral filter
Additional optical isolation (where used)
Active phase / polarisation / intensity modulator(s)
Photon detection

Figure 2: Overview of receiver protection

Attenuators and optical isolators may be inserted to protect transmitter modules. Receiver modules operating some protocols may in appropriate implementations obtain protection by introducing a sufficient length of optical fibre, to act as a delay line with the receiver module, without needing to insert additional optical isolation.

5 System design and input protection

5.1 General design considerations

When designing a QKD system to be safe against Trojan horse attacks it is generally important to minimise reflections from components and interfaces in the quantum channel. Reflections from any active optical component and anything beyond it, when considering access from the entrance port for the quantum channel, should be minimised. It is therefore desirable to use low reflectivity fibre connectors or where possible to splice connections.

During construction it can be beneficial to measure the reflectivity of components and connections to ensure unnecessary reflections are not introduced.

A spectral filter shall be included in the quantum channel just inside the security boundary of the module. This shall attenuate light outside of the operating wavelength range to limit how much light can enter the module. The spectral filter shall be characterised over all wavelengths for which the optical fibre it designed to transmit light. Attenuation within the optical fibre of the quantum channel from the security boundary of the QKD module to the position of the first component (active and passive components shall all be considered here other than the optical fibre itself and the position of the first component shall be determined by considering the system after any additional optical isolation has been introduced) other than the spectral filter may be considered to be part of the function of the spectral filter.

All optical fibre within the DUT should be single-mode for all relevant wavelengths passed by the spectral filter.

All components involved in protecting the system should be designed to fail safely on exposure to excessive optical radiation. For example, the spectral filter should fail to higher attenuation on application of optical powers capable of burning the wavelength selective element(s). Alternatively the protective performance of critical elements should be verified during the exchange of each block of key data with such verification being completed before the corresponding block is trusted.

While a range of active methods may also be considered to detect Trojan horse attacks these introduce significant additional complexity to a system and to the analysis of its security and can introduce additional risks if incorrectly engineered. Implementing such methods safely is beyond the scope of this document and active protection methods shall not be considered under this specification to contribute towards the required protection.

5.2 Designing secure receivers

Much of the power of Trojan horse attacks against transmitter modules arises from the ability of an eavesdropper to make use of information extracted from the transmitter to act on photons in the quantum channel before they enter the security boundary of the legitimate receiver. Receiver modules in unidirectional QKD systems operating certain protocols and meeting certain conditions need not offer an eavesdropper the opportunity to launch such attacks using information obtained from its own active optical components.

In the case of some protocols, such as the unmodified BB84 protocol, information about the basis state selected by the receiver may be revealed publicly after the photons have been measured without compromising the security of the key material.

The presence of a length of optical fibre within the quantum channel inside the receiver module's security boundary can enforce a time delay for information travelling in the quantum channel from the internal active optical elements to the quantum port on the security boundary. So long as the useful lifetime of such information to an adversary is shorter than the delay enforced upon it a fibre delay can offer protection against this type of Trojan horse attack.

The length of optical fibre from the position in the quantum channel at which photons cross the security boundary delimiting the protected region of the receiver module to the first active optical component in the receiver (i.e. the active optical component for which light could arrive with the shortest delay after crossing the security boundary in the quantum channel) shall introduce a delay that is at least as long as the largest of:

1) twice the period between optical signals in the quantum channel;
2) five times the 10% to 90% transition time of the slowest active optical component in the system;
3) five times the 90% to 10% transition time of the slowest active optical component in the system;
4) the useful lifetime of information from any active optical component to an adversary.

The delay of said optical fibre shall be calculated as its length divided by the speed of light in vacuum (not the anticipated speed of light in the optical fibre in case this is modified at high optical powers, for example).

If relying on protection from a fibre delay the active optical components shall be set to an appropriately selected value in each period of the optical signals in the quantum channel and should be set to random values for at least two periods after (before) stopping (starting) key transfer to ensure information that could potentially be useful to an adversary is not present on the active optical components outside of the acceptable duration.

Only receiver modules using protocols and implementations where the useful lifetime of information from any internal active optical component can be bounded shall be regarded as gaining any protection against Trojan horse attacks as a result of an optical delay that meets the specification described in this clause. In other modules optical isolation shall be used to protect receivers.

5.3 Specific considerations for transmitters

Only reflections that cause light that have interacted with active optical components to escape from the security perimeter of the module will present a risk of information leakage via a Trojan horse attack. Optical Time Domain Reflectometry is a technique that can temporarily resolve reflected light from a pulsed source and in this manner it should be possible to identify some reflections as from before the first active optical component in the DUT. It will not always be possible to exclude all reflections from before the first active optical component in the DUT due to the presence of multiple paths and multiple reflections.

The relevant reflectivity is an upper bound on the reflectivity excluding light that can be determined by photon counting OTDR as described in this section to be from before the first active optical component in the DUT.

Protection against Trojan horse attacks shall be achieved from optical isolation in the quantum channel. In many cases the necessary additional protection can be achieved simply and at relatively low-cost by introducing optical isolators into the quantum channel just inside the security boundary of the transmitter module with only modest additional losses.

For example, optical isolators in optical fibre are readily available at common communications wavelengths with > 65 dB of optical isolation being available from commercial devices at 1550 nm in the backward direction with losses of less than 0.4 dB in the forward direction.

A transmitter module may include a variable attenuator that can be reduced during reflectivity measurements below its normal operating value in order to improve the signal to noise ratio for small reflectivities. During normal operation the transmission through this component shall be T_{vA} times the transmission of this component during reflectivity measurements. Such a variable attenuator shall be located in the quantum channel inside the security boundary for the transmitter module beyond the other input protection and before the first active optical component involved in setting the basis or bit values or intensities of transmitted pulses when viewed from outside the security boundary.

6 Measured internal reflectivity

6.1 Additional optical isolation

In order to establish a sufficiently low bound on the relevant reflectivity without requiring the use of intense optical signals the measured internal reflectivity shall be determined in the absence of some amount of additional optical isolation that will be included in completed modules. The amount of additional isolation required depends on the requirements of the module as well as the reflectivity measurement.

In a receiver module where protection is being derived from a delay line additional optical isolation is not necessarily relevant under this specification.

Clauses 6.2 to 6.5 define procedures that shall be followed to establish the measured internal reflectivity and are to be performed in the absence of the additional optical isolation. The transmission of the additional optical isolation T_{AOI} shall be measured as the product of the forward and reverse transmissions of the additional optical isolation. Each of the forward and reverse transmissions shall be measured using the substitution method [2]. The additional optical isolation shall be characterised at all relevant wavelengths and the maximum value determined for T_{AOI} shall be used.

6.2 Common requirements

6.2.1 General precautions

For all reflectivity measurements the common requirements defined in Clause 6.2 and its sub-clauses shall be taken.

Fibres within the test setup should be secured to prevent movement during the test procedures apart from where they need to be moved to make or break a connection. Where connections have to be made during a measurement procedure the entire measurement procedure shall be repeated multiples times (a minimum of 10 times) and the end facet of each connector shall be inspected and cleaned regularly over the period in which the procedure is repeatedly performed. If evidence of any dirt or damage is visible at any stage or if inconsistent results are observed the results shall not be trusted and the entire set of repeated measurements shall be performed again after cleaning or replacing the fibre or fibres impacted. The coupler used to make or break a connection during any measurement procedure shall also be inspected for damage each time and substituted for a different coupler at least twice during the set of repeats and the entire set of measurement shall not be trusted if there is any evidence of a problem with the coupler.

Laser driving conditions shall be set to appropriate values at the start of the measurements at a given wavelength and not adjusted until the complete set of measurement at the given wavelength have been completed. The laser shall be operated well above its lasing threshold to obtain an output state that is a good approximation to a coherent state. This is to reduce variations in laser output parameters, such as pulse width. The laser, detector, electronic delay and all other components shall be designed to be stable to within 5% in all operating parameters and shall be operated within their specified environmental and other operating conditions. Before use the laser, detector, electronic delay and all other components shall be allowed to warm up thoroughly and reach a stable operating state. Its output power shall be verified to be remain stable to within 5% before use by monitoring it on a power meter for as long as will be required to perform the complete measurement procedure.

This procedure shall only apply to QKD modules where the module does not include any optical fibre other than fibre that is single-mode optical fibre and / or polarisation-maintaining single-mode optical fibre at all wavelengths under test.

The optical fibre type used in the measurement setup shall match the type used in the QKD module as closely as possible and shall all be single-mode optical fibre and / or polarisation-maintaining single-mode optical fibre at all wavelengths under test.

At high powers non-linear effects can result in additional losses. All measurements should be undertaken at powers below those where non-linear effects become significant.

6.2.2 Measuring multiple polarisations

The response of the module to different polarisations may be quite different. In particular the path through the optics and the amount of light the active components are exposed to may be very dependent on the polarisation of optical radiation used to probe the system.

Where a transmitter is designed to launch different signals into different polarisation states in the quantum channel the reflectivity of the transmitter shall be probed for each polarisation state used and the maximum of all such reflectivities shall be taken for the transmitter reflectivity. Where a transmitter is designed to launch into a single polarisation state in the quantum channel it shall be probed for this polarisation state and the polarisations state orthogonal to this and the maximum of the two transmitter reflectivities shall be taken.

For any other transmitter a characterisation of the reflectivity over the full Poincaré sphere shall be performed and the maximum reflectivity shall be taken. Reasonable steps sizes on the surface of the Poincaré sphere shall be taken such that all large features are detected and changes between any adjacent measurement positions do not differ by more than 10%. Poissonian noise due to finite numbers of counts may be ignored but the conditions used (source intensity, integration time etc.) shall each be the same as for the reflectivity measurement taken at the maximum.

Where different time delays are introduced for different polarisation states in the quantum channel time-resolved measurements of optical signals that have passed through one or more of the paths for the different polarisations may be used to align test equipment to each polarisation state in turn.

In order to make measurements in a polarisation state the fibres and environmental conditions shall be stable enough that the polarisation state can be set and once set it shall remain stable for long enough for the required measurements to be performed without significant drift in the test polarisation state. Any fraction of the light that may be in the incorrect polarisation state at the end of the measurement shall be accounted for as a measurement error equal to the maximum fraction of light that could have been in the incorrect polarisation state during any part of the measurement.

6.3 No reflectivity characterisation

The measured internal reflectivity r_{mi} may be taken to be unity to avoid the need to perform a reflectivity measurement. $r_{mi} = 1$ will normally be significantly higher than what will be determined in a reflectivity measurement. However, where a sufficient combination of additional attenuation and additional optical isolation are present the resulting additional privacy amplification that assuming $r_{mi} = 1$ will required may not justify performing the reflectivity measurement.

6.4 Basic reflectivity characterisation

A basic characterisation of the measured internal reflectivity may be performed as defined below. Where reflections from before the first active optical component are not small a basic characterisation may overestimate the relevant reflectivity and result in a stronger requirement from privacy amplification than may be necessary and worse overall performance. In some situations using a basic characterisation can prevent a secure key material from being produced. Single photon OTDR measurements may always be performed to exclude reflections that are not relevant to Trojan horse attacks.

TODO: Decide whether to permit this and if so insert or reference detailed procedure.

6.5 Single photon OTDR measurement procedure

6.5.1 Experimental set up for test measurements

The following arrangement shall be constructed for test measurements where the laser source is sent to the detector via optical circulator port 2. The optical circulator shall be designed to transmit light from port 1 to port 2 and from port 2 to port 3.

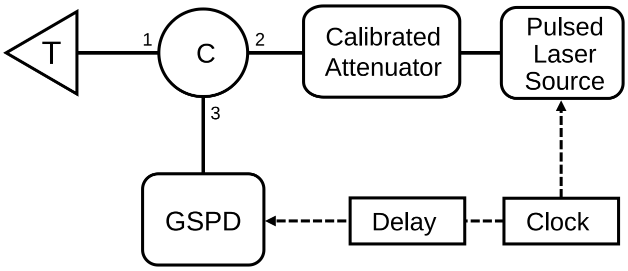

Figure 3: Measurement setup for GSPD gate scan

In Figure 3 dotted lines connecting components represent signals that may be of any type including electrical and solid lines connecting components represent optical fibres. C is a fibre optic directional coupler and T is a non-reflecting terminator. It shall be possible to vary the delay in equal steps of a size as determined in clause 6.5.6. It shall be confirmed that changing the delay does not alter the frequency of the GSPD (e.g., if the delay is increased above the period of the clock).

A variable time delay may optionally be inserted between the clock and the pulsed laser source. In this case it shall be confirmed that changing the delay does not alter the frequency of the pulsed laser source (e.g., if the delay is increased above the period of the clock). If the pulsed laser source is delayed the resulting OTDR results that are recorded shall be reversed to indicate early and late reflections appropriately.

6.5.2 Confirming linearity of the gated single photon detector

The power range over which the single photon detector is linear (after correction for dark counts to within 5% should be verified according to the measurement procedure in Clause 16 of [1] or the corresponding procedure in any future update to [1]. If it is confirmed to be linear to the required level up to the maximum power to be used in the measurement the upper bound to its linear response need not be determined.

6.5.3 Laser power considerations

The laser power shall be operated well above threshold and an attenuator or attenuators used to reduce the power if necessary. High laser powers will be beneficial in terms of signal to noise ratio but the laser power shall not be high enough to cause the light incident on the GSPD during any gate period to exceed that for which the GSPD was found to have a linear response under clause 6.5.2. Additionally the power shall not be high enough to generate a count rate that causes a long-term change to the response of the detector following removal of the reflected light e.g. due to heating. The power shall low enough to avoid any significant non-linear processes within the optical fibre or any optical component.

The laser source shall include sufficient optical isolation to prevent instability or significant modification to its output due to reflected light during any of the measurements at the chosen power. Instead or as well as using a lower laser power additional optical isolation may optionally be added in front of the laser to meet this requirement.

6.5.4 Interference effects

The test operator shall ensure that the reflectivity is not underestimated due to any potential destructive interferences that could occur during the test measurements. Short laser pulses shall be used for all reflectivity measurements and each optical pulse shall have a random phase with respect to any other laser pulse in the measurement. One or more of the following additional approaches shall also be used:

- **design**: all fibre lengths within the QKD module and test equipment should be designed to avoid unnecessary interference of optical pulses of the duration used during the test measurements. A table of optical delays between interfaces in the quantum optical path within the QKD module may be compiled. From this the timings of the arrival of potentially significant pulses at various interfaces can be checked to establish whether they are separated by more than the duration of the test optical pulses.
- **active modulation**: where active elements that are able to introduce phase changes are present in one or more paths within the QKD module these may be rapidly swept during the test measurements such that an average between constructive and destructive interference would be measured within the duration of any measurement. The sweep rates may determine the minimum integration time required for an individual time step in an OTDR measurement such that the average reasonably samples all phases. The module reflectivity shall be taken to be twice the measured reflectivity if this approach is used.

- **thermal modulation**: where only polarisation-maintaining fibre is present within the QKD module such that polarisation evolution as a result of temperature changes is not an issue rapid temperature variation may be used to induce phase changes in one or more paths within the QKD module. If used, it will often be desirable for such phase changes to be rapid. The rate of such phase changes may determine the minimum integration time required for an individual time step in an OTDR measurement. The module reflectivity shall be taken to be twice the measured reflectivity if this approach is used.
- **path attenuation via knots**: in OTDR measurements where potential for interference exists due to light in two fibre paths a 'knot' may be used within each fibre in turn to attenuate light in that path. A 'knot' may for example be one or more loops around a cylindrical core or a knot such as a clove hitch around a cylindrical core such that the 'knot' is of a diameter and length that attenuates optical signals within the fibre path by e.g. at least two orders of magnitude without significantly affecting the fibre once removed. The reflectivity for each step in the OTDR trace shall be taken as twice the maximum of:
    - the signal with both paths unattenuated;
    - the signal with each 'knot' or combination of 'knots'.

6.5.5 Determining an appropriate OTDR source period

The frequency of the OTDR source shall be sufficiently low that the time period between source pulses is not less than 5 times the maximum propagation time through the longest direct optical fibre path within the DUT. This is to allow for multiple reflections to be captured.

The longest direct optical fibre path shall be taken to mean a direct optical path within the system under test without considering reflections unless the system includes any reflective components or interfaces with reflectivities greater than 0.1. If any such components are present the longest direct optical fibre path within the DUT shall also consider any additional paths formed by reflections from such intentionally reflective components and truncated only where the product of the reflectivities of multiple reflections from such components or interfaces becomes less than 0.01.

6.5.6 Determining an appropriate OTDR delay step size

A scan shall first be taken by stepping delay of the laser source relative to the gate of the gated single photon detector using the measurement setup shown in Figure 3. The delay step size shall be adjusted to be sufficient small as to reliably capture the shape of the response function of the GSPD and any features in the laser pulse profile. The step size shall be small enough to ensure that the statistically significant variation in count rate measured between adjacent data points is no more than 5% of the maximum mean count rate measured when the laser pulse and detector gate are optimally aligned in time. Poissonian noise due to finite numbers of counts may be ignored but the laser intensity used shall be sufficient to give at least as many counts for the maximum delay as will be detected for any time delay in the final reflectivity measurement.

6.5.7 Efficiency calibration OTDR scan for known laser intensity

The same setup as in Figure 3 shall be used for the efficiency calibration OTDR scan.

A laser of known intensity shall be used to calibrate the detector. A calibrated attenuator shall be used to attenuate the laser source down to a level that can be recorded using the single photon detector. This attenuation may be reduced by a calibrated amount during the OTDR measurement of the QKD module in order to measure small reflectivities with sufficient accuracy. The calibrated attenuator shall be tested to ensure that the two attenuation values it produces for the chosen high- and low-attenuation settings are reproducible to within 5% over each of at least 20 cycles. The calibrated attenuator shall only be set alternately to the high- and low-attenuation values from the start of these 20 cycles through to the end of the final OTDR measurement to avoid any errors relating to hysteresis.

The transmission corresponding to the difference between the high-attenuation setting $T_{\mathrm{SA\_high}}$ and the low-attenuation setting $T_{\mathrm{SA\_low}}$ shall be calculated as:

$$T_{\mathrm{SA}} = T_{\mathrm{SA\_high}} / T_{\mathrm{SA\_low}}. \qquad (1)$$

The transmission of the fibre optic direction coupler T_{12} shall be measured using the substitution method [2].

The relative delay between the laser and the gate of the single photon detector shall be stepped using a uniform step size and the count rate shall be recorded as a function of this delay for the known laser power passing through the directional coupler from port 2 to 3. The appropriate OTDR step size determined in clause 6.5.6 shall be used and the integration time for each delay shall be chosen to be appropriate to achieve an appropriate level of accuracy in both this scan and the OTDR measurement of the DUT. (If the integration time is too low the resulting error will result in a significantly higher bound on the relevant reflectivity than is necessary.) After changing the delay the system shall be allow to reach a steady state before starting the integration time during which detector events are collected. The scan range shall cover a full period of the laser source and the number of counts within the chosen integration time shall be recorded for each step.

6.5.8 Determining the detector dark count rate

The average number of detection events within the integration time shall be recorded in the absence of illumination on the GSPD. The pulsed laser source shall be disconnected for this measurement and it shall be ensured that ambient light is not able to reach the GSPD. Any disconnected ends of optical fibres leading to the GSPD shall be capped using metal caps and all optical fibres leading to the GSPD shall be isolated from ambient light using an enclosure or dark room.

The number of detection event within the integration period shall be measured in the absence of illumination on the GSPD shall be measured multiple times and an average value D calculated. This average value may include some afterpulses due to previous dark counts but no correction shall be made.

6.5.9 Performing an OTDR scan

The experimental arrangement shown in Figure 4 shall be used to perform the OTDR scan of the QKD module under test (the DUT). Where components are indicated that are also present in Figure 3 the same actual components shall be used. Settings such as those of the pulsed laser source shall not have been altered since performing the efficiency calibration scan as described in clause 6.5.7. In this case the laser source is introduced to port 1 of the directional coupler and passes to the DUT attached to port 2. Light reflected from the DUT is passed to the gated single photon detector, which remains connected to port 3 of the directional coupler.

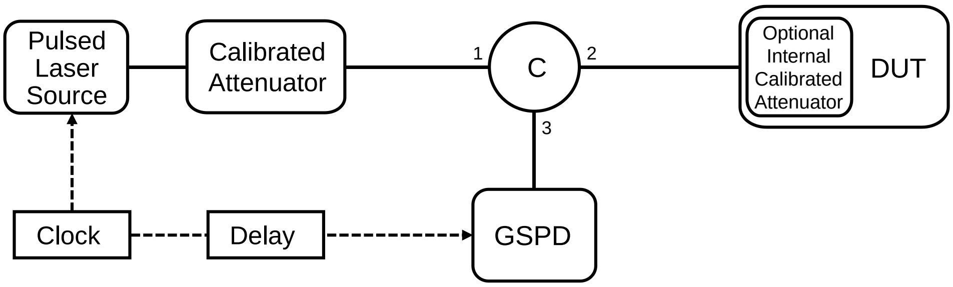

Figure 4: OTDR measurement setup

In Figure 4 dotted lines connecting components represent signals that may be electrical and solid lines connecting components represent optical fibres. C is a fibre optic directional coupler.

The relative delay between the laser and the gate of the single photon detector shall be stepped using the same uniform time step as the efficiency calibration OTDR scan (clause 6.5.7) and the count rate shall be recorded as a function of this delay.

If the wavelength, laser source parameters or single photon detector parameters etc. are altered the procedures described in clause 6.5 shall be repeated to ensure a consistent set of measurements.

The OTDR scan shall cover a range of time delays covering a full period of the pulsed laser source. The data shall be taken to be periodic in the period of the pulsed laser source.

The results are likely to show a series of peaks from internal interfaces within the DUT as well as other counts that are likely to be more spread out in time due to effects such as light scattered within the fibre, dark counts and detector afterpulsing. Depending on the measurement equipment, some closely space interfaces may not be fully resolved. The main peaks should be identified from knowledge of the fibre lengths between components in the system and if any uncertainty remains repeating the scan with strategically placed knots in fibres to attenuate the signals from particular interfaces may be used to confirm any uncertain assignments.

Each time delay step shall be indicated by integer index that increases by one between each step corresponding to a later reflection (consider whether the pulsed laser source or GSPD is being delayed).

The OTDR scan shall be repeated for different polarisation states as required by clause 6.2.2.

The time delay corresponding to the earliest reflection from the first active optical component in the module (i.e. the active optical component for which light could arrive with the shortest delay after crossing the security boundary in the quantum channel) shall be identified. The range of steps that are to be considered to contribute to the relevant reflectivity shall start at s where s corresponds to the step at least 5 times the FWHM detector gate width earlier than the time delay corresponding to the earliest reflection from the first active optical component in the module. The range of steps that are to be considered to contribute to the relevant reflectivity shall finish at f where f corresponds to the step at least 5 times the FWHM detector gate width before the first reflection due to the subsequent laser pulse.

The total number of detector events contributing to the relevant reflectivity shall be calculated by summing the counts for time steps s to f :

$$C_{DUT} = \sum_{n=s}^{f} c_{DUT}(n\delta). \tag{2}$$

A similar sum shall be taken for the scan recorded during the efficiency calibration OTDR scan. In this case the start of the sum s' shall correspond to the step at least 5 times the FWHM detector gate width earlier than the peak of the signal from the pulsed laser and the number of steps included in the sum shall be the same as for C_{DUT} :

$$C_{cal} = \sum_{n=s'}^{f-s+s'} c_{cal}(n\delta). \tag{3}$$

The measured internal reflectivity shall be calculated as:

$$r_{mi} = \frac{C_{DUT} - D\times(f-s+1)}{C_{cal} - D\times(f-s+1)} \times \frac{T_{SA}}{T_{12}}. \tag{4}$$

Broad background signal may arise from scattering within the optical fibre. These photons shall be included as dangerous in the security analysis where they are at times suggesting a position that would indicate them to be relevant reflectivity. Only dark counts and afterpulses may be corrected for in the total summed counts.

7 Bounding the reflected mean photon number

The relevant reflectivity can be calculated as:

$$r_{rel} = r_{mi} \times T_{vA} \times T_{AOI}. \tag{5}$$

A justification shall be recorded in the technical file for the number of photons μ_{in} that could be injected into a module per state prepared by the transmitter before the injected power would render the module non-functional. This justification might be based on the damage threshold of a length of optical fibre inserted into the quantum channel inside the security boundary of the system and before any active optical components. The bound should be based on a failure mechanism for a physical component such as damage to a length of fibre or a particular passive optical component in the quantum optical path inside the security boundary of the module but before any active optical component.

The upper bound on the mean photon number of Trojan horse photons μ_{out} shall be calculated according to:

$$\mu_{\text{out}} \le \mu_{\text{in}} \times r_{\text{rel}}. \tag{6}$$

8 Privacy amplification requirements

The upper bound on μ_{out} determined according to the procedures above shall be used in conjunction with information about the protocol in operation, its implementation in the system, parameters in use and data obtained during operation of the module to determine the amount of privacy amplification that shall be applied to the shared key material with the objective of removing information that may have been obtained by an adversary via a Trojan horse attack on the system. Privacy amplification shall then be applied to the shared key material accordingly.

The adopter shall provide a security justification for how they calculate the amount of privacy amplification they perform. The analysis used shall either be publicly available and referenced in the technical file or included in the technical file.

The justification shall:

- provide an expression for or a procedure to calculate the amount of privacy amplification to be applied to protect the system from a Trojan horse attack on the active bit-encoding polarisation or phase modulators in the system based on the upper bound to the reflected photon intensity μ_{out} as determined using measurements described elsewhere in this document;
- include a reasonably detailed description of the methodology adopted such that it could be understood and assessed by a person experienced in the field;
- be reasonably comprehensive and shall not ignore aspects of current understanding that would be reasonably regarded as important by those experienced in the field;
- state the main assumptions underlying the justification;
- take account of any multi-photon emission from the photon source(s) and any methods used to mitigate them, such as decoy pulses, and the analysis of transmission / error rates that may be used to bound potential attacks by an eavesdropper due to the presence of multi-photon emissions and how such analysis relates to measured parameters;
- consider the finite size of the blocks of key material upon which privacy amplification is performed.

Systems operating the BB84 protocol and variations of this protocol were considered when this document was written. Implementers are free to use any protocol to which the approach of using a bound on μ_{out} in the manner discussed can be applied so long as they provide an appropriate security justification. Additional measurements may be defined if necessary.

Joint attacks including a Trojan horse attack in combination with another attack or information from an independent side channel are not explicitly considered in this document but these may be included within the security justification. In this case any additional measurements that may be necessary will need to be defined to take account of the other attacks. Nonlinear optical effects within QKD modules are not explicitly considered in this document. If relevant to the security justification additional measurements may be defined if required.

9 Record keeping

Details relating to the design of a specified model of QKD module that has adopted this specification shall be kept by the manufacturer in a technical file along with details of relevant tests that were performed as part of the validation of the design. The technical file shall be retained for the expected lifetime of the modules produced under the design.

The following details shall be recorded when specifying that protection is compliant with this specification:

- Details of the protocol to be used and its implementation;
- A schematic diagram showing the optical layout of the QKD module;
- Details of the optical components in the system and their relevant optical specifications;
- The type of optical fibre(s) using within the QKD module and their locations;
- The method used for optical connections between components (e.g. which are spliced and the type and specifications of any pluggable connectors used);
- Schematic diagrams, procedures followed and parameters used in any relevant measurements;
- The serial number(s) of the QKD module(s) and / or component(s) used in any relevant measurements;
- Details of additional equipment used in any relevant measurements. Where relevant to security details may include the model number, serial number(s), specification and calibration information;
- The wavelength(s) over which any relevant measurements were preformed;
- The power level(s) used in any relevant measurements;
- The upper bound taken for the mean photon number μ_{in} and the justification for the adoption of this bound;
- A copy of or reference to a security justification for how the amount of privacy amplification performed is determined;
- Quality control measures to be implemented in the production of modules produced under the design.

Annex A (informative): Authors & contributors

The following people have contributed to this specification:

Rapporteur:
Dr., Martin, Ward, Toshiba Research Europe Ltd.

Other contributors:
TODO: Add list of contributors after review by members

Annex B (informative): Bibliography

- A. Vakhitov, V. Makarov, and D. R. Hjelme, “Large Pulse Attack as a Method of Conventional Optical Eavesdropping in Quantum Cryptography”, J. Mod. Opt. **48**, 2023 (2001).

- A. Winick, N. Lütkenhaus, and P. J. Coles, “Reliable numerical key rates for quantum key distribution” arXiv:1710.05511v1 (2017).

- D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, “Security of quantum key distribution with imperfect devices” Quantum Inf. Comput. **4**, 325 (2004).

- H.-K. Lo, X. Ma, and K. Chen, “Decoy State Quantum Key Distribution”, Phys. Rev. Lett. **94**, 230504 (2005).

- ISO 21254:2011 “Lasers and laser-related equipment — Test methods for laser-induced damage threshold”.

- K. Tamaki, M. Curty, and M. Lucamarini, “Decoy-state quantum key distribution with a leaky source” New J. Phys. **18**, 065008 (2016).

- K. Tamaki, M. Koashi, and N. Imoto, “Unconditionally Secure Key Distribution Based on Two Nonorthogonal States” Phys. Rev. Lett. **90**, 167904 (2003).

- K. Tamaki, M. Koashi, and N. Imoto, “Loss-tolerant quantum cryptography with imperfect sources” Phys. Rev. A **90**, 052314 (2014).

- M. Koashi, “Efficient Quantum Key Distribution with Practical Sources and Detectors”, arXiv:quant-ph/0609180.

- 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).

- N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, “Trojan-Horse Attacks on Quantum-Key-Distribution Systems”, Phys. Rev. A **73**, 022320 (2006).

- N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, “Risk Analysis of Trojan-Horse Attacks on Practical Quantum Key Distribution Systems” IEEE J. Sel. Top. Quantum Electron. **21**, 6600710 (2015).

- N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, “Trojan-horse attacks threaten the security of practical quantum cryptography” New J. Phys. **16** 123030 (2014).

- P. J. Coles, E. M. Metodiev, and N. Lütkenhaus. “Numerical approach for unstructured quantum key distribution” Nature Communications 7:11712 (2016).

- S. Sajeed, C. Minshull, N. Jain, and V. Makarov, “Invisible Trojan-horse attack” Scientific Reports **7**, Article number: 8403 (2017).

- S. Sajeed, I. Radchenko, S. Kaiser, J.-P. Bourgoin, A. Pappa, L. Monat, M. Legré, and V. Makarov, “Attacks exploiting deviation of mean photon number in quantum key distribution and coin tossing” Phys. Rev. A **91**, 032326 (2015).

Annex C (informative): Change History

Date	Version	Information about changes
December 2017	0.0.1	Early draft (released to open area on Docbox)

History

Document history		