Draft ETSI GS QKD 010 V0.4.1 (2021-06)

GROUP SPECIFICATION

Quantum Key Distribution (QKD); Implementation security: protection against Trojan horse attacks

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Do not cite this document other than as "work in progress".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

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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 specifies protection of QKD modules against Trojan horse attacks launched against a time-varying phase, polarisation or intensity modulator that encodes or decodes at least one of bit values, basis values or the intensities of signal, decoy or vacuum states from the quantum channel.

The present document is applicable to Trojan horse attacks involving attempts by an adversary to obtain information about the state of one or more time-varying phase, polarisation or intensity modulator that resides within the security boundary of a QKD transmitter module or a QKD receiver module. It is applicable to attacks in which information is leaked to an adversary by optical radiation exiting the security boundary of the QKD module through the quantum channel, where the optical radiation carrying the leaked information had previously been inserted into the same QKD module by the adversary via the same interface.

The present document is applicable to the design, measurement and operation of QKD modules operating discrete variable QKD protocols (including those using decoy states) where the interface of the QKD module to the quantum channel comprises an optical fibre that is designed to transmit only a single transverse optical mode at the operating wavelength(s) of the system.

The present document is not directly applicable to QKD modules in which the quantum channel is multiplexed with other quantum or classical signals internal to the security boundary of the QKD module. However, the present document is applicable to a subset of many such systems within an appropriately chosen internal security boundary.

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 https://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".

2.2 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]	IEC 60793-1-40:2019: "Optical fibres — Part 1–40: Attenuation measurement methods".

3 Definitions, symbols and abbreviations

3.1 Terms

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 forms 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 module where optical radiation is inserted by an adversary into apparatus under the control of a legitimate sender and / or receiver in order to measure information about the state of active optical components internal to the QKD module

EXAMPLE: Optical pulses might be inserted into the quantum port of a phase-modulated QKD transmitter module. 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. This could enabling the adversary to know how to measure bit values from the signal photons emitted by the QKD module. In some systems the phase of reflected photons might contain information about the bit values transmitted.

NOTE 1: The optical radiation enters the QKD module via the normal quantum channel interface for the entry / exit of photons used for key establishment. Information is leaked back to the adversary through a portion of the previously inserted optical radiation exiting the apparatus via the normal quantum channel interface.

NOTE 2: The adversary may combine the information leaked in this manner with information intentionally encoded on either the quantum or classical channels by the QKD module. Any attempt by the adversary to interfere with the operation of the QKD module or to combine information from a Trojan horse attack with information from any other side-channel would be considered a joint 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
$r_p^{'}$	The number of photons reflected in the p-th reflectivity peak in…
r_p	The number of photons returning from the p-th interface in…
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 6.4.2) 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 6.4.2)
$T_{\text{SA\_low}}$	Transmission of the calibrated optical attenuator in its low-attenuation setting as used for OTDR scans on the DUT (see clause 6.4.9)
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} is 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 the present document to protecting QKD modules against Trojan horse attacks starts by determining an upper bound to the optical power that could be usefully inserted into the module by an adversary. This may be based on the damage threshold(s) of at least one component of the module, such as optical fibre within the security boundary of the module.

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 the 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 reduce the risk an adversary has information about the final key to below a chosen value.

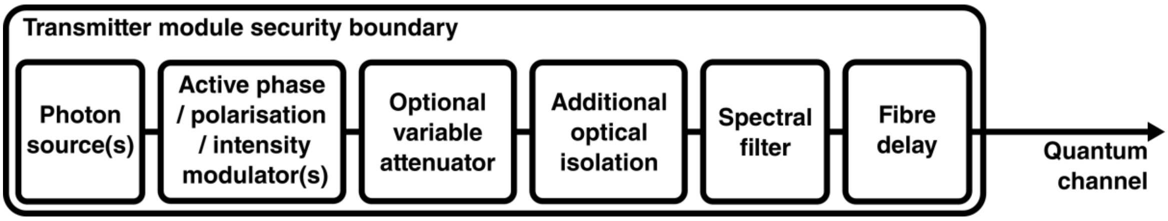
Transmitter module security boundary
Photon source(s)
Active phase / polarisation / intensity modulator(s)
Optional variable attenuator
Additional optical isolation
Spectral filter
Fibre delay
Quantum channel

Figure 1: Overview of transmitter protection

Attenuators and optical isolators may both be inserted as additional optical isolation to protect transmitter modules without impacting performance in many weak-laser-pulse QKD transmitter modules. Attenuators will degrade performance of QKD transmitter modules using single-photon sources much more than optical isolators.

Receiver modules operating some protocols may in appropriate implementations introduce a sufficient length of optical fibre to act as an optical delay within the receiver module, without needing to insert additional optical isolation. See clause 5.2 for details. Optical isolation may also be used to protect receiver modules.

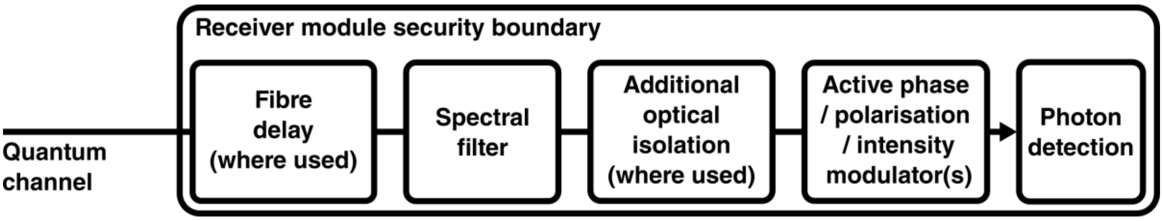
Receiver module security boundary
Quantum channel
Fibre delay (where used)
Spectral filter
Additional optical isolation (where used)
Active phase / polarisation / intensity modulator(s)
Photon detection

Figure 2: Overview of receiver protection

5 System design and input protection

5.1 General design considerations

When designing a QKD system to offer protection against Trojan horse attacks and high performance it is generally important to minimise reflections from components and interfaces in the internal paths carrying quantum signals. 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 splice connections or to use low reflectivity fibre connectors.

During construction it can be beneficial to measure the reflectivity of components and connections to avoid introducing unnecessarily strong reflections.

A spectral filter shall be included in the quantum channel within the security boundary of all QKD transmitters and receivers. The spectral filter should attenuate light outside of the intended operating wavelength range(s) of the QKD module. It should provide appropriate attenuation over all wavelengths ranges where it is being relied upon for protection. The design of the filter should be analysed and any additional passbands at non-operating wavelengths should be considered. Multiple optical filters may be used in series to provide the necessary protection jointly. Attenuation within the quantum channel from the security boundary of the QKD module to the first component being protected (passive as well as active components should be considered) may be considered 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.

The components involved in protecting the system should be designed to act together to ensure that protection is not compromised upon exposure to excessive optical radiation. For example, the spectral filter could be designed to fail to a high attenuation state on application of optical powers capable of burning the wavelength selective element(s). Active monitoring of protection may be used if necessary. Any such active monitoring should be designed to be resistant to influence from an adversary and verification during the exchange of each block of key data should be completed before the corresponding block is trusted.

While a range of active methods could also be considered to detect Trojan horse attacks as the direct protection mechanism these introduce significant additional complexity and additional risks if incorrectly implemented. Implementing such methods safely and their security analysis is beyond the scope of this document. Active protection methods shall not be considered to contribute towards the required protection under this specification apart from monitoring passive protection measures for integrity.

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 adversary the opportunity to launch attacks using information obtained from its 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 Trojan horse attacks on such receiver modules.

To rely upon such an optical delay for protection 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 to an adversary of information from any active optical component in the system.

The delay of such 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).

Receiver modules using protocols and implementations where it is not possible to bound the useful lifetime of information from any internal active optical component shall not 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 has 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. 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 where multiple paths and multiple reflections are present.

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

A QKD 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 is T_{vA} times the transmission of this component during reflectivity measurements. Where used, such a variable attenuator shall be located in the quantum channel inside the security boundary for the QKD transmitter module beyond the other input protection and before the first active optical component involved in setting the basis, bit or intensity values 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 6.4 define procedures 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, for example, the substitution method [i.1]. The additional optical isolation shall be characterised at all relevant wavelengths and the maximum value determined for T_{AOI} shall be used. It should be ensured that the claimed T_{AOI} protection is not compromised on application of powers up to the upper bound to the optical power that could usefully be inserted into the module by an adversary.

6.2 Common requirements

6.2.1 General precautions

For all reflectivity measurements the general precautions defined in Clause 6.2 and its sub-clauses should be implemented.

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(s) 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. The entire set of measurement shall not be trusted if there is 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 suitably stable in all relevant 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 sufficiently stable before use by monitoring it on a power meter for as long as will be required to perform the complete measurement procedure.

QKD modules shall 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 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 Single photon OTDR measurement procedure

6.4.1 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.

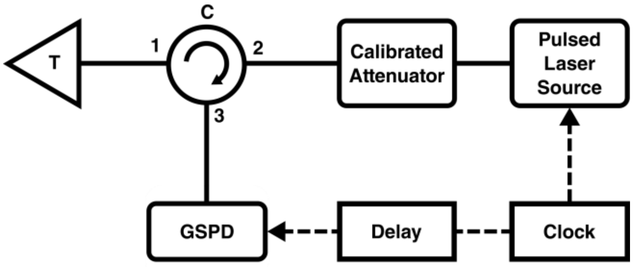

Figure 3: Measurement setup for GSPD gate scan

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 terminator that is non-reflecting to a high degree. It shall be possible to vary the delay in equal steps of a size as determined in clause 6.4.6. 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.

6.4.2 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.

6.4.3 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 6.4.2. 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.

6.4.4 Interference effects during reflectivity characterisation

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'.

6.4.5 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.

6.4.6 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.

6.4.7 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:

$$T_{\mathrm{SA}} = T_{\mathrm{SA\_high}} / T_{\mathrm{SA\_low}}. \tag{1}$$

The transmission of the fibre optic direction coupler T_{12} shall be measured, for example, using the substitution method [i.1].

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 6.4.6 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.

6.4.8 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.

6.4.9 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 6.4.7. 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.

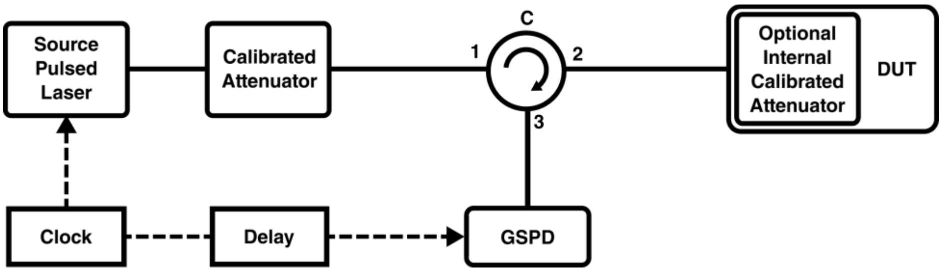

Figure 4: OTDR measurement setup

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 6.4.7) 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 6.4 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 range of steps that are to be considered to contribute to the relevant reflectivity shall start at s and finish at f. s shall correspond 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. f shall correspond to the last step to occur less than one OTDR source period after s. Note that the OTDR source period shall have been determined according to 6.4.5 to ensure that strong multiple reflections return within this period.

It is assumed that all reflections could return in-phase and coincident in time resulting in constructive interference so the total number of detector events contributing to the relevant reflectivity shall be calculated by summing the counts for time steps s to f:

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

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}:

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

The measured internal reflectivity shall be calculated as:

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

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

7.1 Attacks exploiting interference

7.1.1 Interference during attacks

Clause 6.4.4 warns of the potential for interference during the characterisation of a module reducing the measured reflectivity and includes guidance to help identify any such interference. In bounding the reflected mean photon number the potential for interference to increase the reflected mean photon number during an attack shall also be considered.

The illumination that an attacker can use in a Trojan horse attack is assumed to be limited only by the optics of the quantum channel, including protections such as the spectral filter. In the following clauses two specific cases are considered: constant coherent laser illumination and targeted pulse interference.

7.1.2 Constant coherent laser illumination

If constant coherent laser illumination is applied there is scope for constructive interference between the reflections from different positions. The phase relation between the reflected light from different positions in the optical path can vary from being close to stable through to strongly time varying. Reflections from surfaces that are close together on a stable substrate with no active elements between them, such as those within a dielectric stack forming a coating on a component, can have a very stable phase relation between them for light of wavelengths that can pass through the spectral filter. The phase relation between light reflected from interfaces separated by a long length of fibre can be subject to variation with temperature, vibration etc.

A simple analysis to calculate an upper bound for the light potentially reflected back in this type of attack would be to consider that all reflected light returns in phase. For a system with many interfaces of similar reflectivity it would be extremely unlikely that by chance all reflected light would return exactly in phase at any given time. However, if all phase differences were randomly time varying then some degree of constructive interference would be expected half of the time with the variations tending to be strongest when the number of highly reflecting interfaces is small.

It should also be considered whether or not an attacker could find a mechanism to actively alter certain phase differences e.g. by causing heating of a component. This would be a combined attack involving additional control of the module in combination with a Trojan horse attack and is out of the scope of the present document.

7.1.3 Targeted pulse interference

An attacker could insert a series of coherent optical pulses timed to ensure that for each pulse the reflection from a different interface reflects back through the targeted active component at the same time. Such pulses would interfere and the case of most interest is where the attacker sets the phase of each inserted pulse to ensure that all the pulses reflecting back through the targeted active component at the same time are in-phase with each other to achieve fully constructive interference.

It is important to note that each input pulse also reflects from all the other interfaces in the optical path so only a fraction of the reflected illumination returns at the same time to undergo interference. The other reflections return at different times.

7.2 Identifying reflectivity peaks

Each clear peak in the time-resolved reflectivity data shall be identified and the number of photons it represents shall be estimated. This may be done by fitting each peak taking into account the known response function of the detection system to short laser pulses. Where a peak is found to be significantly wider than the expected response function or a different shape it may be fitted with the multiple peaks. Any known information about the positions of interfaces etc. giving rise to reflections may be taken into account to constrain fits.

Where the reflections from the front and rear interfaces of a component are not temporally resolved in the reflectivity data it shall be assumed that there are two reflectivity peaks of equal intensity unless further information is available about the component enabling a better estimate of the ratio of the two reflections.

Surfaces that are extremely close together and where the phase difference between reflections from these surfaces is expected to be highly stable, e.g. within a dielectric antireflection coating on a component, may be treated as generating a single reflectivity peak.

7.3 Calculating the interference-modified internal reflectivity

Each of the identified reflectivity peaks shall be treated as being due to a reflecting interface.

The number of photons reflected in each identified reflectivity peak are estimated as $r_p$where p is the index of the reflectivity peak starting with $p = 1$ for the most delayed peak identified with p increasing for reflectivity peaks through to $p = P$ for the first relevant reflection. The number of photons returning from an interface p is denoted r'_p.

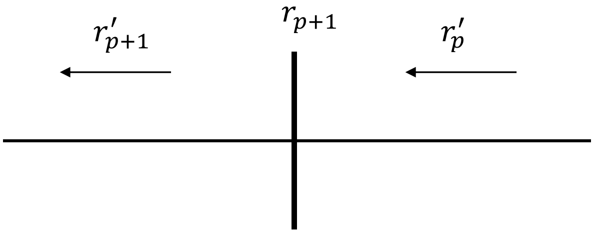

Figure 5: Interference at a reflecting interface

The number of photons returning from interface $p + 1$ shall be determined as:

$$r'_{p+1} = \left(\sqrt{r'_p} + \sqrt{r_{p+1}}\right)^2. \tag{5}$$

The calculation shall begin with the most distant peak from the security boundary. For each closer reflecting interface in turn the total number of photons returning shall be calculated assuming fully constructive interference between the reflection from the interface and the total reflected from all more distant interfaces calculated in the previous step. Ultimately the interference-modified internal reflectivity due to the peaks shall be the total reflected intensity calculated in the final step r'_P for the first relevant reflecting surface given by:

$$r'_P = \left(\sum_{p=1}^{P} \sqrt{r_p}\right)^2. \tag{6}$$

Temporally broad reflectivity, for example that due to backscatter in optical fibre, may be considered not to be involved in any interference. The measured internal reflectivity less the sum of all the individual identified reflectivity peak intensities (not modified for interference) shall be added to the interference-modified internal reflectivity due to the peaks to give the overall interference-modified internal reflectivity.

More detailed modelling of the physical implementation of a QKD module and the possible interference within it may be used to calculate a tighter upper bound on the reflected photon number.

7.4 Upper bounding the mean photon number of reflected photons

The relevant reflectivity can be calculated as:

$$r_{\mathrm{rel}} = \left(r_{\mathrm{mi}} - \sum_{p=1}^{P} r_p + r'_P\right) \times T_{\mathrm{vA}} \times T_{\mathrm{AOI}}. \tag{7}$$

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 reflected photons exiting the module μ_{out} shall be calculated according to:

$$\mu_{\mathrm{out}} \leq \mu_{\mathrm{in}} \times r_{\mathrm{rel}}. \tag{8}$$

8 Security modelling and privacy amplification

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.

Editorial note: It was agreed to add information about possible security models to implementation security work items. This section contains initial draft text that has not yet been reviewed by the ISG.

In QKD modules that are protected by strong optical isolation, relevant reflections of bright probe signals from internal components will be heavily attenuated by the time they exit the QKD module. Strong attenuation of any quantum state brings it closer to a low-intensity coherent state, ultimately tending towards a vacuum state that is not squeezed. It is not anticipated that using arbitrary quantum states in a Trojan horse attack upon such a system would be likely to give an adversary a strong advantage over using coherent states.

The coherent state intensities could be varied in a security model but it is not anticipated that the adversary will be advantaged by varying the intensity of the coherent states in time, beyond interference effects that could impact μ_{out} as considered in clause 7, so continuous wave coherent states may be considered.

At least for transmitter modules where the emitted pulses are independent from each other, the bright probe states sent in by an adversary are from an external independent source. For the security analysis of a Trojan horse attack upon such a transmitter module that is protected by strong optical isolation, the overall states emerging from the transmitter module may therefore be described as tensor products of the QKD states emitted under the QKD protocol and independent coherent states that — in the conservative limit — have also been encoded with the maximal information they could potentially have obtained from the active components within the transmitter module.

For example, in the case of such a transmitter module operating a phase-encoded qubit-based BB84 protocol the states exiting the transmitter module could modelled as

$$|\Psi_{\mathrm{out}}\rangle = \frac{1}{\sqrt{2}}\left(|1\rangle_{\mathrm{long}}|0\rangle_{\mathrm{short}} + e^{-i\varphi}|0\rangle_{\mathrm{long}}|1\rangle_{\mathrm{short}}\right) \otimes \left|e^{-i\varphi}\sqrt{\mu_{\mathrm{out}}}\right\rangle \quad (9)$$

where $|n\rangle_{\mathrm{long/short}}$ represents an n-photon state exiting the long/short arm of the encoding part of the interferometer, $\sqrt{\mu_{\mathrm{out}}}$ represents the attenuated reflection of an independent coherent state of mean photon number μ_{out}, and φ is the encoded phase difference, which would take values from $\{0,\ \pi,\ \pi/2,\ 3\pi/2\}$ in a typical 4-state BB84 protocol.

In many protocols, pulses emitted from an interferometer are only independent from each other for time differences above some value. Inclusion of an optical delay within the transmitter module that is sufficiently long to ensure that QKD signal pulses in the active components of the transmitter module are independent from probe signals an attacker could have prepared from previously emitted pulses would be sufficient to enable the tensor product above to be considered in such cases.

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 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 $\mu_{in}$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.

10 Measurements during the life cycle of a QKD module

10.1 Development and manufacturing

Measurements of the additional optical isolation will be a part of the development and manufacturing phases of QKD modules. Where protection relies upon measurement of internal reflectivities rather than, e.g., assuming unity reflectivity, this will also involve measurements during the development and manufacturing phases of QKD modules.

Based on the design of a QKD module and the quality control procedures in place during manufacture a developer may decide whether it is appropriate to measure part(s) of a sample of QKD modules or every QKD module manufactured. A developer may also decide the stage(s) of development and manufacture at which measurements are performed. These decisions should ensure that QKD modules that pass the quality control procedures in place during manufacture include at least the intended level of protection.

Choices may be influenced by the design of the QKD module since some measurements may not be possible on production devices where components are inseparable (e.g. in some chip designs). In such cases testing of additional optical isolation may be performed on specially made devices including specific part(s) of the QKD module. Where it is necessary to use such specially made devices they shall be designed to be as similar as possible to the corresponding component used in the QKD module and appropriate precautions shall be taken to ensure that they will behave under test in a manner that is representative of the corresponding component used in the QKD module.

10.2 Pre-operational and operational phases

Following manufacture, the whole of the remaining full life cycle of QKD modules should be considered through to destruction. For example, if a QKD module were involved in a traffic accident during delivery it might be necessary to send the QKD module for re-evaluation before bringing it into operation. Shock indicators might be used when shipping a QKD module to detect mishandling in excess of the specifications.

The behaviour of an individual optical fibre is typically rather stable (aside from reversible drifts in length, birefringence etc.) where used inside a protective housing but if the design of a QKD module is believed to be susceptible to changes in its internal reflectivities or variations in additional optical isolation over time (beyond interference effects that are discussed in other clauses) then it should be considered whether a there is a need to perform periodic remeasurement of relevant part(s) of the QKD module.

10.3 Remeasurement

Remeasurement of a QKD module may be performed in any suitable location (e.g., in the field, factory or test laboratory etc.). Any remeasurement shall be performed by a competent trusted. If adjustment of system parameters is required rather than pass/fail testing then this shall be considered a calibration activity with appropriate procedures and access controls etc. If internal access is required to the QKD module or the removal or disassembly of security features then an appropriate secure procedure shall be specified and followed.

Annex A (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).

History

Document history		
V0.0.1	December 2017	Initial draft released to open area on Docbox.
V0.2.1	June 2020	Draft released to open area on Docbox.
V0.4.1	June 2021	Draft released to open area on Docbox including: title revised to remove “one-way”, scope wording aligned with changes and drafting rules, internal reflectivity analysis updated to consider interference, new text on modelling, new clause on measurements during life cycle of QKD module, figures redrawn and equations converted to internal Word format.