INTERNATIONAL STANDARD

ISO/IEC 23837-2

First edition
2023-09

Information security — Security requirements, test and evaluation methods for quantum key distribution —

Part 2: Evaluation and testing methods

Sécurité de l'information — Exigences de sécurité, méthodes d'essais et d'évaluation relatives à la distribution quantique de clés —

Partie 2: Méthodes d'essais et d'évaluation

Reference number
ISO/IEC 23837-2:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 23837 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

The ISO/IEC 23837 series specifies security requirements, test and evaluation methods for quantum key distribution (QKD) modules under the framework of the ISO/IEC 15408 series. This document specifies an evaluation method and relevant evaluation activities for the security evaluation of QKD modules in a relatively general way. The evaluation activities that are necessary for the security evaluation of QKD modules include supplementary evaluation activities for the QKD-related security functional requirements (SFRs) specified in ISO/IEC 23837-1 and the supplementary evaluation activities for security assurance requirements (SARs) with security assurance levels ranging from evaluation assurance level (EAL) 1 to EAL 5+.

Specifically, the evaluation activities for the testing and evaluation of implementations of QKD protocols, quantum optical components in QKD transmitter modules, and QKD receiver modules are described in detail. For SFRs specific to conventional network components, this document does not specify concrete evaluation activities but mainly refers to existing methods for network devices. In addition, supplementary activities for security assurance requirements are specified, and refinements to the generic vulnerability analysis methodology in ISO/IEC 18045 are presented, including guidance on the calculation of attack potentials.

This document is expected to provide a specification to help QKD manufacturers improve the design and implementation security of QKD modules, and to guide evaluators in the testing and security evaluation of QKD modules, thus reducing the risk of failure of security in operation.

Information security — Security requirements, test and evaluation methods for quantum key distribution —

Part 2: Evaluation and testing methods

1 Scope

This document specifies test and evaluation methods for the security evaluation of quantum key distribution (QKD). It also describes evaluation activities that constitute the test and evaluation methods for the security functional requirements on the implementation of QKD protocols, the quantum optical components and conventional network components in QKD modules. Moreover, supplementary evaluation activities for security assurance requirements are provided to support the security evaluation of QKD with appropriate assurance levels.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408-4:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities*

ISO/IEC 18045, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation*

ISO/IEC 23837-1:2023, *Information security — Security requirements, test and evaluation methods for quantum key distribution — Part 1: Requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 23837-1 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
attenuation
reduction in the intensity of a light beam relative to the distance travelled through a transmission medium

3.2
attenuator
device used to reduce the power level of a light beam

3.3
back-flash
pulse of one or more photons emitted from a single-photon detector

Note 1 to entry: This phenomenon is also known as “backflash light” or “breakdown flash”.

Note 2 to entry: This phenomenon is due to radiative charge recombination, and is observed in devices such as avalanche photodiodes where large populations of electron-hole pairs are created.

3.4
beam splitter
BS
device which can split an incident light beam at a designed ratio into two or more separate beams

3.5
correlation function
function used to characterize the statistical and coherence properties of light beams

3.6
dark count
detection event registered by an optical detector in the absence of optical illumination

3.7
dead time
time interval after a detection event when the detector as a whole is unable to provide an output in response to incoming photons at the single photon level

[SOURCE: ETSI GR QKD 007 V1.1.1:2018]

3.8
density matrix
matrix that describes the state of a quantum system

3.9
detection probability
probability that a detector registers a detection event within a stated duration time

3.10
emulator
tool with a known and trusted implementation of the expected functionality under test

3.11
fidelity
measure of the closeness of two quantum states

3.12
injected light monitor
detector for monitoring the power of the laser light injected from the quantum channel

3.13
local oscillator
LO
strong optical signal that acts as a phase reference for interference with a weak optical signal (e.g., quantum state) in coherent detection

3.14
mean photon number
average number of photons per optical pulse

[SOURCE: ETSI GR QKD 007 V1.1.1:2018]

3.15
polarization
property of electromagnetic waves that describes the orientation of the oscillating electric field vector

[SOURCE: ETSI GR QKD 007 V1.1.1:2018]

3.16
polarization analyser
instrument designed to measure and display the *polarization* (3.15) of an optical pulse

3.17
quantum state analyser
instrument designed to measure optical states in one or more specified degrees of freedom

3.18
shot noise
noise which can be modelled by a Poisson process, describing the fluctuations of the number of photons detected due to their occurrence independent of each other

3.19
spectrum analyser
instrument designed to measure and display the distribution of power of an optical source over a specified wavelength span

4 Abbreviated terms

ATE	assurance class of tests
AVA	assurance class of vulnerability assessment
cPP	collaborative PP
EA	evaluation activity
EAL	evaluation assurance level
EM	evaluation method
IT	information technology
NRBG	non-deterministic random bit generator
PP	protection profile
QKD	quantum key distribution
RX	receiver
SAR	security assurance requirement
SFR	security functional requirement
SPD	single-photon detector
TOE	target of evaluation
TSF	TOE security functionality
TSFI	TSF interface
TX	Transmitter

5 Overview of the evaluation method for QKD modules

5.1 General

The primary objective of the security evaluation of QKD modules is to validate whether the implementation of the core functionality and the IT-related security controls of QKD modules meet the security requirements of an expected evaluation assurance level (EAL).

Since the high-level generic evaluation activities (EAs) specified in ISO/IEC 18045 do not directly cover all aspects of the security evaluation of QKD modules, this document gives an evaluation method (EM) to supplement ISO/IEC 18045, by considering the characteristics of QKD modules. In particular, this EM includes some specific EAs for security functional requirements (SFRs), which are defined in ISO/IEC 23837-1, and security assurance requirements (SARs), which are defined or refined based on the work units in ISO/IEC 18045.

5.2 Scope of the evaluation method

The defined method for the security evaluation of QKD modules is based on the framework specified by ISO/IEC 15408-4. Figure 1 gives the structure of the EM based on the following considerations.

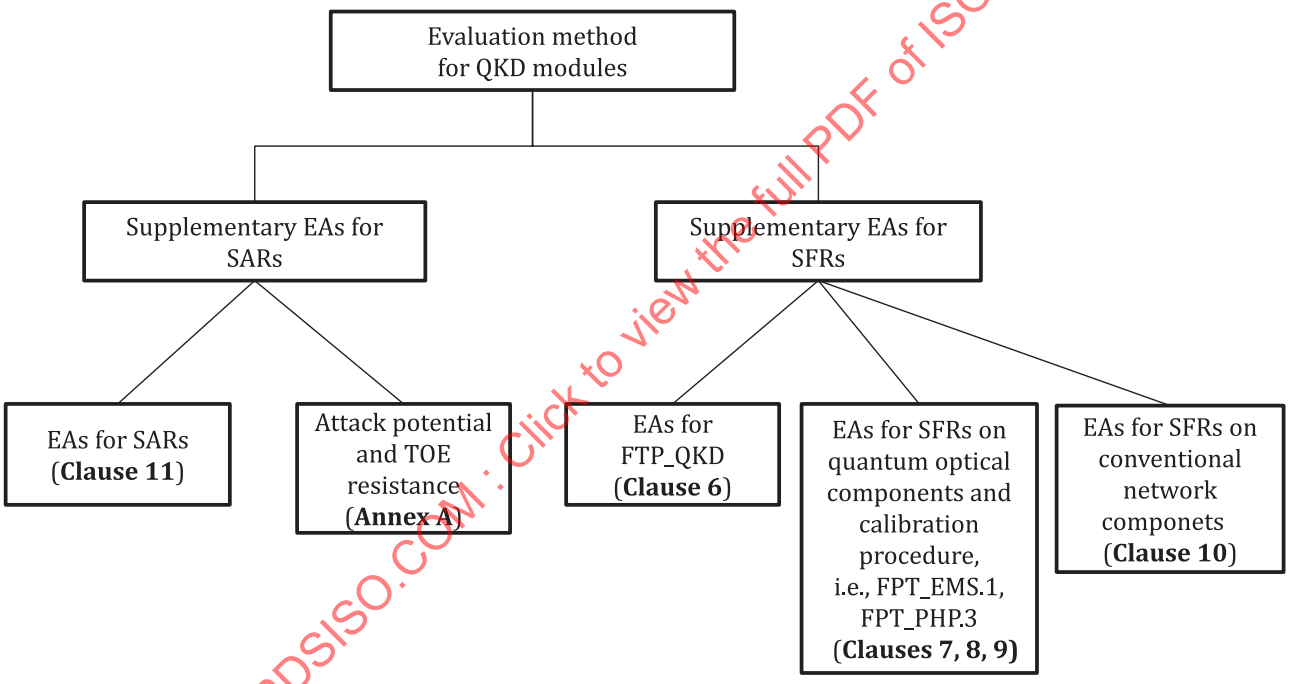


Figure 1 — Structure of the specific EM for QKD modules and its constituent EAs

The EM includes a collection of EAs for SARs and SFRs. In particular, a set of EAs for some existing SARs in ISO/IEC 18045 are supplemented to make their work units more specific for the evaluation of QKD modules, in particular those related to the assurance Class ATE and Class AVA (see 11.6, 11.7 and Annex A). In addition, a set of EAs for specific SFRs is defined, which addresses SFRs on the quantum optical components (see ISO/IEC 23837-1:2023, 9.4) and the implementation of QKD protocols (i.e. FTP_QKD). The EAs for SFRs are intended to help evaluators address evaluation actions required by the SARs ATE_IND.1 and ATE_IND.2 that are specific to QKD modules (see Clauses 6 to 9 for further detail).

On the other hand, since the objective of this document is to provide a supplementary evaluation methodology that is specific to QKD modules, EAs for common SFRs on conventional network components (including SFRs in the classes of FCS, FIA, FDP, FMT defined in ISO/IEC 15408-2) are not emphasized. As the corresponding methodology for those SFRs is relatively mature in the IT security evaluation industry, evaluators may reference existing standards or methodologies to handle

such aspects. Clause 10 explains this in more detail, and existing standards and methodologies are referenced to help evaluators select appropriate approaches.

Not all EAs in this document are required for the security evaluation of a specific TOE of QKD modules. The selection of EAs depends on the implemented QKD protocols and the implementation strategy of the TOE. Clause 12 describes the requirements of the conformance statement when a specific evaluation process claims conformance with this document.

5.3 Overview of evaluation activities for SFRs

5.3.1 General

The objective of functional testing in a security evaluation is to verify whether the implementation of the functionality and IT-related controls are consistent with the design specification, and that the security requirements defined in the ST are satisfied by the TOE. The EAs for SFRs, as specified mainly in Clauses 6, 7, 8, and 9, are intended to supplement the work units concerned with independent functional testing of the TSF, especially the work units regarding the security assurance family of ATE_IND in ISO/IEC 18045.

NOTE This includes the work units of ATE_IND.1–3, ATE_IND.1–4, ATE_IND.1–5, ATE_IND.1–6 and ATE_IND.1–7 when ATE_IND.1 is chosen for the expected EAL, or the work units of ATE_IND.2–6, ATE_IND.2–7, ATE_IND.2–8, ATE_IND.2–9 and ATE_IND.2–10 when ATE_IND.2 is chosen.

Although the EAs are intended to help evaluators of QKD modules, these EAs can also be used to help developers of QKD modules perform functional testing (for security assurance family of ATE_FUN), and ensure the evaluator that the tests have been performed and documented correctly, before applying for security evaluation/certification.

ISO/IEC 15408-4:2022, Clause 6 explains that the content generally required for the specification of an EA includes:

— objective of the evaluation activity;

— required inputs (from the developer);

— required tool types and setup;

— required evaluator competence;

— rationale (justification of their derivation from the work units in ISO/IEC 18045);

— dependencies (of the activities on other relevant EAs);

— test procedure (for performing the EA);

— pass/fail criteria (for deciding the outcome of the EA).

Regarding these EAs, the general inputs required by the evaluator (but mainly prepared by the developers) for independent testing are defined in ISO/IEC 18045, and include at least:

a) if ATE_IND.1 is concerned in the evaluation, then the following inputs are required:

— the ST;

— the functional specification;

— the guidance documentation;

— the TOE suitable for testing;

b) if ATE_IND.2 is concerned in the evaluation, then the following additional evidence is required:

— the TOE design description;

— the configuration management documentation;

— the test documentation.

In addition, all the test tools required for the EAs shall be calibrated correctly against some specific standards by default. Otherwise, the reason shall be justified in the corresponding EAs.

For each EA, it is necessary for the developer to present at least the general inputs listed in a) and b) accordingly to the evaluator. On completion of the evaluation process, the evaluator shall report the evaluation result of the EA.

The "dependencies" item specified in ISO/IEC 15408-4:2022, Clause 6 is not necessary for the description of EAs that are independent of all other EAs. The item is therefore neglected from the description of those EAs hereinafter.

5.3.2 EAs for SFRs FTP_QKD.1 and FTP_QKD.2

ISO/IEC 23837-1 defines an extended security functional family (i.e. FTP_QKD) to specify the requirements on the FUN_QKD functionality (see ISO/IEC 23837-1:2023, 6.4.2 for the definition) of QKD modules. Correspondingly, EAs related to the evaluation of the implementation of a QKD protocol, or rather the implementation of raw data generation, post-processing and parameter adjustment procedures are specified in 6.2, 6.3, and 6.4 respectively. These EAs are used to examine the correctness of the implementation of FUN_QKD (or more precisely, the SFRs FTP_QKD.1 and FTP_QKD.2).

Each of the EAs provides the required content listed in 5.3.1, especially the following:

a) Test procedures for checking the correctness of the implementation of raw data generation, post-processing and parameter adjustment procedure(s) of the TOE.

b) Pass/fail criteria (for the evaluation of an implementation of a QKD protocol).

5.3.3 EAs for SFRs on quantum optical components and parameter adjustment procedure(s)

The SFRs on quantum optical components and parameter adjustment procedure(s) mainly include FPT_EMS.1/Quantum and FPT_PHP.3 (see ISO/IEC 23837-1:2023, 9.4). These requirements are imposed on the relevant security functions that relate to quantum optical components of QKD modules and the parameter adjustment procedure(s). The expectation is that, at the expected EAL, the TOE that meets these SFRs can resist known attacks (mainly) conducted from the quantum channel.

This document describes EAs for the two SFRs representing the parts of a QKD evaluation that are most specific to QKD technology-specific evaluation activities, and are the focus of this document (see Clauses 7, 8, and 9). The common objective of these EAs is to help an evaluator examine the effectiveness of the IT-related controls used by QKD modules to resist known attacks.

Such EAs specify the required content listed in 5.3.1, especially the following:

a) Test procedures for checking the correctness of the implementation of IT-related controls employed by the QKD modules to address the identified threats to quantum optical components and the parameter adjustment procedure(s).

b) The pass/fail criteria, pertaining to each EA related to quantum optical components and the parameter adjustment procedure(s). The following considerations are related to the criteria:

   1) In some cases, effective IT-controls against some known attacks (related to the threats to quantum optical components) are well studied and recognized in the community, and vulnerabilities related to those attacks cannot be exploited if corresponding IT-controls have been adopted. The pass/fail criteria for these cases are explained as whether relevant IT-controls have been effectively implemented in the TOE. For example, the EA in 8.11 examines the ability of the TOE to resist double-click attacks, and the test passes if appropriate measures have been adopted and implemented.

2) In some cases, the security of the TOE is connected with some security-related technical parameters. That is, when the values of certain parameters exceed (or are less than) certain thresholds, it is possible the TOE includes some vulnerabilities that can be exploited by the adversary. In such cases, test procedures provide methods to measure concrete values for the parameters by examining the TOE. The pass/fail criteria in such EAs generally specify comparisons with given thresholds as the method to decide the evaluation result. For example, the EAs in 7.8, 7.9 and 8.4 examine the ability of the optical isolation component and the injected light monitor of the TOE, and make pass/fail verdicts based on the measured values of relevant parameters.

3) In some cases, the measured security-related technical parameters described in 2) can be incorporated into the privacy amplification process of the post-processing procedure to address the problem of potential information leakage caused by potential vulnerabilities. Where a developer claims to be doing so, after performing these EAs, the evaluator should also examine whether the thresholds used by the pass/fail criteria are correctly used in the privacy amplification process of the TOE. An example of these cases is the EA in 8.2.

EAs for these SFRs usually involve performing tests over some pre-defined parameter spaces specified by the input parameters of the EAs. Since most of the parameter spaces are continuous, this document adopts the strategy of evenly discretizing the parameter spaces and performing the test step by step. Alternatively, the tests may be performed by randomly probing the parameter space (such as in the EAs of 7.9, 8.5, 8.9, and 9.2).

With regard to performing tests for the EAs, evaluators shall take account of measurement errors. The normal objective is to ensure that sufficient data are measured to demonstrate that tests are passed in a statistically significant manner. However, in some EAs, the parameters shall be scanned in a range that may include regions where the probability of measuring events falls close to zero, such as near the edges of the active window of a gated detector. In such cases, it is not practical to measure sufficient data to ensure tests pass reliably over the entire range. Where appropriate, evaluators may state that such a test only fails if a pass/fail criterion is failed in a statistically significant manner after a reasonable amount of data has been recorded.

To clearly understand the relationship between EAs and known attacks against the QKD modules, see Table D.1.

5.3.4 EAs for SFRs on conventional network components

The evaluation of conventional network components is a relatively mature topic in the security evaluation community for conventional network devices. In order to remove unnecessary complexity and retain consistency with the methodologies in existing standards, this document does not define new evaluation activities for conventional network components unless necessary, and refers to existing standards or specifications wherever possible. The SFRs within the classes of FAU, FCS, FDP, FIA, and FMT, pertaining to the evaluation of security audit, cryptographic operation, RNG, and network-management functions respectively, can typically be evaluated by referring to existing methods, including those from ISO/IEC 18367, ISO/IEC 20543 and cPP for Network Devices.[6] See Clause 10 for further information.

5.3.5 Thresholds and input parameters related to the evaluation activities

For most of the EAs specified in this document, thresholds and input parameters have been defined in the test procedures and are used to specify the pass/fail criteria and the input constraints. The thresholds, input parameters, and relevant pass/fail criteria together constitute the basis for the evaluator issuing an evaluation verdict and shall be a necessary part of the evaluation method of QKD modules.

Since the primary objective of the document is to specify the general evaluation method for QKD modules, this document does not specify values for the thresholds and input parameters. Instead, the values of thresholds and input parameters are expected to be given in PPs, STs or anywhere recognized by the relevant evaluation authority. Specifically, they can be specified according to the expected

EAL of the evaluation. An evaluation authority can provide requirement(s) upon such values to the stakeholders (including the evaluators, developers, and users of QKD modules).

Tables C.1 and C.2 illustrate the thresholds distributed among the EAs.

As a convention of this document, the allowable ranges for some input parameters are described in the form of closed intervals, i.e. [*a*, *b*], where *a* and *b* are exact values depending on the context. For example, a tunable laser with a wavelength λ in the range of $[\lambda_{min}, \lambda_{max}]$ means $\lambda_{min} \leq \lambda \leq \lambda_{max}$.

5.4 Overview of evaluation activities for SARs

The evaluator shall carry out a set of work units as specified in ISO/IEC 18045 to reach a verdict for the evaluation related to the assurance classes, families, and components (see ISO/IEC 15408-3). For security evaluation of QKD modules, supplementary evaluation activities are defined to make those generic work units described in ISO/IEC 18045 more specific by noting the characteristics of QKD modules, as described in Clause 11 in detail.

In principle, to meet the needs of the whole stack of pre-defined assurance levels from EAL 1 to EAL 7, all standardized assurance components specified in ISO/IEC 15408-3 should be scrutinized to supplement new evaluation activities for the evaluation of QKD modules. This document confines itself to only dealing with levels from EAL 1 to EAL 5+, where the augmentation of the security assurance component mainly focuses on AVA_VAN.5.

6 EAs for the evaluation of FTP_QKD

6.1 General

The SFRs on QKD protocol implementation are characterized by the extended functional family FTP_QKD, which captures the security requirements of the two essential stages of raw data generation (FTP_QKD.1) and post-processing (FTP_QKD.2). The EAs shown in Table 1 mainly focus upon the following aspects, with the general objective of examining the correctness of an implementation of the FUN_QKD functionality (or specifically the SFRs of FTP_QKD.1 and FTP_QKD.2):

— raw data generation;

— post-processing;

— parameter adjustment.

Table 1 — EAs for the evaluation of FTP_QKD

Evaluation activity	Description	SFRs correspondence	Subclause index	Applicable protocols
Test quantum state transmission and sifting procedures	Test the correctness of functionality of the related generation of raw data between the TX module and the RX module, and the functionality of sifting of the resulting data when sifting is part of the QKD protocol.	FTP_QKD.1 FTP_QKD.2	6.2	DV-PM-QKD; DV-MDI-QKD; DV-EB-QKD; CV-PM-QKD; CV-MDI-QKD; CV-EB-QKD
Test other post-processing procedures	Test the correctness of the implementation of the post-processing procedures in the TOE, subsequent to any sifting that forms part of the QKD protocol.	FTP_QKD.2	6.3	DV-PM-QKD; DV-MDI-QKD; DV-EB-QKD; CV-PM-QKD; CV-MDI-QKD; CV-EB-QKD
Test parameter adjustment procedure(s)	Test the correctness of the implementation of the parameter adjustment procedure(s) in the TOE.	FTP_QKD.1	6.4	DV-PM-QKD; DV-MDI-QKD; DV-EB-QKD; CV-PM-QKD; CV-MDI-QKD; CV-EB-QKD

The general requirements for carrying out these activities are as follows:

— required inputs in general, as described in 5.3.1;

— required tool types and setup in general: quantum channel related measurement equipment, network sniffer tools, post-processing emulator;

— required evaluator competences in general: the evaluator for this kind of EAs should be an expert in the optical measurements area;

— dependencies (in general): some of the EAs for FTP_QKD depend on the EAs for FPT_EMS.1/Quantum and FPT_PHP.3, which are detailed in Clauses 7, 8, and 9.

NOTE More specific requirements for each EA are added in 6.2 to 6.4 accordingly.

More information about the test and description of these EAs is given as follows:

a) Ideally, the security test procedures should be conducted on the QKD modules under test as a whole, without any adaptations. The objective of evaluation activities is to establish the security status of actual QKD modules under the conditions they can face in operation. In some instances, however, if the information gained from measuring the whole system is insufficient, it may be necessary to test individual components or sub-assemblies of QKD modules. Specifically, for the test of raw data generation and post-processing functions, the QKD modules under test shall be adapted to output a set of additional digital data to facilitate the access of some intermediates of protocol execution, which are needed to better perform the test, as detailed in the EAs in 6.2 and 6.3.

b) Since the EAs in Clause 6 are intended to test the correctness of the implementation of raw data generation and post-processing procedures, the tests are confined to being performed in an environment without adversarial intervention. More precisely, it is assumed that testing errors or faults that arise from noise were not maliciously introduced by an adversary.

c) For simplicity, the description of EAs in Clauses 6, 7, 8, and 9 mainly consider the implementation of DV-PM-QKD protocols. Although there are obvious differences between types of QKD protocols, the EAs in this document are designed and described in such a general way that:

1) those EAs described on the QKD transmitter modules can also be applied to the implementations of MDI-QKD protocols;

2) those EAs described on QKD receiver modules can also be applied to the implementations of EB-QKD protocols.

The applicability of each EA specified in this document is identified in general in the last column of Table 1 and in similar tables in Clauses 7, 8, and 9.

6.2 EA to test quantum state transmission and sifting procedures

6.2.1 General aspects

a) Objective of the evaluation activity

This EA intends to test the correctness of the functionality of raw data generation between the TX module and the RX module, and the functionality of sifting the resulting data when sifting is part of the QKD protocol. Although other post-processing procedures are evaluated under 6.3, sifting typically handles high data-rates that are comparable to the transmission frequency, so it is considered here.

NOTE The TOE does not include the quantum channel and classical channel connecting the QKD TX module and RX module, but only the relevant interfaces corresponding to the channels, as described in ISO/IEC 23837-1:2023, 6.4.2.

b) Required inputs

Besides the relevant documentation listed in the general input requirements, it is required to adapt the TOE (where not a capability of the TOE) to provide a set of additional digital data in order for the test to be performed. The data rates in the TX module can be high for some additional digital data. In many cases, the additional digital data that shall be output is generated at a rate that is a few times greater than the rate at which quantum states are emitted from the transmitter module, dependent upon the QKD protocol in operation. For this EA, it is sufficient for the TX and RX modules to retain additional digital data for finite durations and deliver these retrospectively to the evaluator. The retained duration may be shorter than the duration of a QKD session. Tests may be repeated where necessary to reduce statistical uncertainty in the results.

c) Required tool types and setup

If the module under test is a QKD transmitter, an RX emulator with known characteristics is required to be available and working well. Similarly, if the module under test is a QKD receiver, a TX emulator with known characteristics is required to be available and working well. An emulator is a tool with a known and trusted implementation of the raw data generation and sifting functionalities, which allows analysis of the TX (or the RX) module under test. In other words, the emulator does not undertake any security requirements, but the correctness of its implementation is expected to be suitable for the analysis of the TX (or the RX) module under test.

To conduct this EA, the evaluator shall have an emulator in advance. The emulator can be prepared by the evaluator or implemented and then provided by the QKD manufacturer or the industrial community for evaluation. Either way, the emulator should be recognized by the evaluation authority.

The schematic of the setup for testing the encoder functionality of the TX module under test is shown in Figure 2. In some implementations, the functionalities of the signal source and encoder may be implemented together rather than as separate components. The schematic of the setup for testing the decoder functionality of the RX module under test is shown in Figure 3. Figure 2 and Figure 3 show just one example of relevant internal components and connections, and implementations can differ. Digital output 3 (as shown in Figures 2 and 3) can be derived from the detector in implementations

using passive techniques for decoding quantum states. The emulator shall provide any signal required by the TX/RX module under test to perform the functions of raw data generation and sifting close to a normal mode of operation.

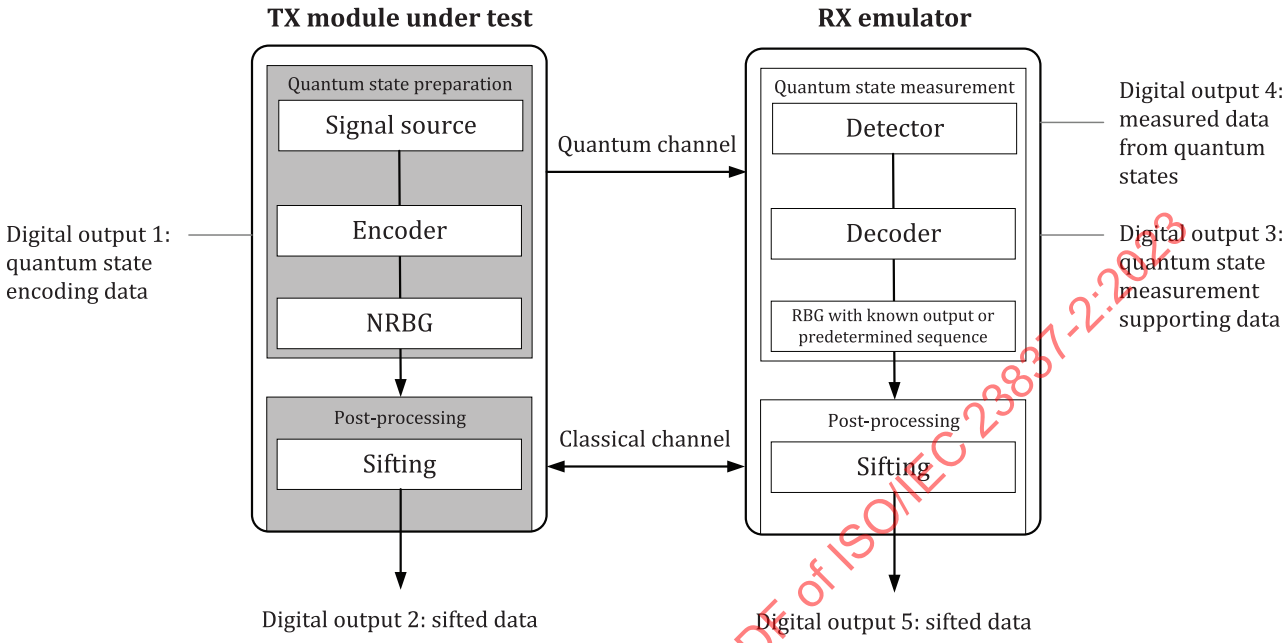


Figure 2 — Setup for testing encoding and sifting functionalities of a TX module

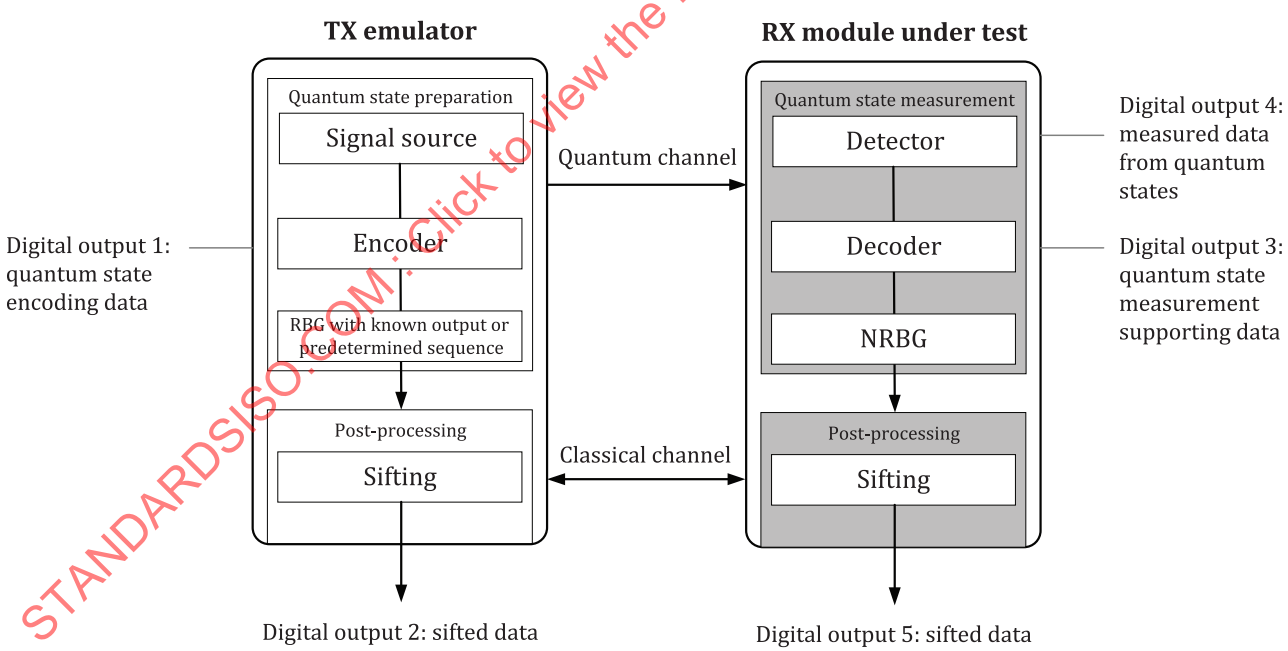


Figure 3 — Setup for testing quantum state measurement and sifting functionalities of an RX module

Figure 2 and Figure 3 do not show the whole structure of the QKD module under test and the emulator, but only the quantum state preparation/measurement and sifting components, since these are targets of the EA. This abstraction does not mean that other components are not necessary for the test. In fact, since the test is conducted on the QKD module under test as a whole, all components inside the QKD module under test are necessary and supposed to be in a normal running state apart from supplying the additional digital data required for the tests, so the results are representative of the real status of an actual QKD module.

While an NRBG is necessary for some protocols, it can be substituted by passive optical devices in others.

d) Rationale

The security of a QKD transmitter module crucially depends on the correct implementation of the protocol through the NRBG, signal source, and encoder. Similarly, the security of a QKD receiver module crucially depends on the correct implementation of the protocol through the NRBG, decoder, and detector. As a first step of the evaluation, it is necessary to examine the correct behaviour of these components in the system. The test procedure is based on knowledge of the random values used for encoding and measurement of quantum states (for relevant protocols). These can be used to determine whether the results of measurements of quantum states are statistically consistent with those expected if the QKD protocol had been implemented correctly within some threshold. By adapting the QKD module under test to allow access to the data used for preparing/measuring quantum states, the effectiveness of raw data generation and sifting functionalities in the module under test can be examined. Considering the typical lengths of the additional digital data that the QKD modules are configured to deliver, an input parameter n_{exe} denoting the execution times shall be assigned before conducting the EA. The input parameter is the number of sets of additional digital data that shall be evaluated for the tests in this EA to be statistically significant.

e) Dependencies

This EA has some dependencies on other EAs, including those on testing signal sources and detectors (see Clauses 7 and 8).

6.2.2 Test procedure

6.2.2.1 QKD transmitter module

NOTE The digital outputs 1 to 5 are shown in Figures 2 and 3.

— Step 1: Prepare the environment for the test and connect the TX module under test and the RX emulator as required to perform the QKD protocol(s) to be evaluated. The initial step is to configure the TX module under test as the protocol requires. If the TX module under test is required to negotiate protocol configurations with its peer before executing the rest of the protocol, this shall be tested with the RX emulator before proceeding to the next step. Such configuration is often performed using purely conventional network components or specific to a protocol, and detailed activities are not discussed here.

— Step 2: Run the functionality under test. The TX module under test outputs from digital output 1 a set of quantum state encoding data that includes the necessary information used to encode quantum states over some test periods. For example, some simple discrete variable protocols that use two orthogonal states in each of two non-orthogonal bases output two bit-strings corresponding to the bit values and basis states used to encode quantum states. These are typically derived from the output of an NRBG. Intensity information is also required in some QKD protocols, such as protocols utilizing decoy states, or in some continuous variable protocols.

  In the RX emulator, any necessary information used to perform each measurement on a quantum state over some test period is made available through digital output 3. The measured data and any necessary timing information are made available through digital output 4. For example, the detector(s) register a photon for each quantum state for which detection occurred and the timings of those events.

— Step 3: Execute step 2 multiple times and accumulate the digital data from all digital outputs until the number of sets of data held is n_{exe}. There may be gaps between the periods when each data set was collected, but each digital data set shall correspond to a consistent set of quantum states. Where there is more than one possible protocol configuration, repeat step 1 between data sets and ensure that all possible protocol configurations are covered during the test. Then end the test. If the number

of configurations is large, an appropriate sampling of configurations may be agreed with the evaluator.

— Step 4: The evaluator should review the quantum state encoding data output from digital output 1 and test whether the distribution of encoded states is consistent with the QKD protocol implemented by each of the protocol configurations tested in step 3. As a minimum, the evaluator shall test that each state occurs with the probably expected for the QKD protocol as configured after considering measurement and statistical errors.

— Step 5: Compare the sifted data from digital output 2 of the TX module under test against the full quantum state encoding data from its digital output 1 using knowledge from digital outputs 3 and 4 of the RX emulator. Test that any sifting required under the QKD protocol was implemented correctly by the TX module under test.

— Step 6: Compare the sifted data from the TX module under test received through digital output 2 with the sifted data from the RX emulator through digital output 5. The expected relationships between elements of the sifted data depends upon the QKD protocol and the evaluator shall test whether the sifted data relates as expected. For example, in many discrete variable protocols, the two sets of sifted data are strongly correlated bit strings, although in many cases, the sifted data from the TX module under test may include additional data, e.g. which quantum states were decoy or vacuum states. In this case, the overlap between the main string of sifted bit values encoded by the TX module under test and the measured sifted bit string from the RX emulator provides a check of whether the intended bit values were encoded. In such cases, the overlap can be calculated as the number of bits in the main sifted bit strings divided by the total length of the main sifted bit strings. More detailed tests of the quality of encoding of the individual quantum states themselves are described in Clause 7.

6.2.2.2 QKD receiver module

— Step 1: Prepare the environment for the test and connect the TX emulator and the RX module under test as required to perform the QKD protocol(s) to be evaluated. The initial step is to configure the RX module as the protocol requires. If the RX module under test needs to negotiate protocol configurations with its peer before executing the rest of the protocol, this shall be tested with the TX emulator before proceeding to the next step. Often such configuration is performed using purely conventional network components or is specific to a protocol and detailed EAs are not discussed here.

— Step 2: Run the functionality under test. The TX emulator outputs from digital output 1 a set of quantum state encoding data that includes the necessary information used to encode quantum states over some test period.

  In the RX module under test, any necessary information used to perform each measurement on a quantum state over some test period should be made available through digital output 3. For example, where an NRBG is used to randomly configure the decoder to measure the quantum state in a protocol using two non-orthogonal bases, the random bit string used to configure the decoder should be output. The measured data itself, along with any necessary timing information, shall be available from digital output 4. For example, the detector(s) register a photon for each quantum state for which detection occurred and the timings of those events.

— Step 3: Execute step 2 multiple times and accumulate the digital data from all digital outputs until the number of sets of data held is n_{exe}. There may be gaps between the periods when each data set was collected, but each digital data set shall correspond to a consistent set of quantum states. Where there is more than one possible protocol configuration, repeat step 1 between data sets and ensure that all possible protocol configurations are covered during the test. If the number of configurations is large, an appropriate sampling of configurations may be agreed with the evaluator.

— Step 4: The evaluator should review the quantum state measurement supporting data output from digital output 3 and test whether the distribution of measurements performed is consistent with the QKD protocol implemented by each of the protocol configurations tested in step 3. As a

minimum, the evaluator shall test that each configuration occurs with the probably expected for the QKD protocol as configured after considering measurement and statistical errors.

— Step 5: Compare the sifted data from digital output 5 of the RX module under test against the full measured data from quantum states from its digital output 4, using knowledge from its digital outputs 3 about the measurements performed and the quantum state encoding data from the TX emulator's digital output 1. Test that any sifting required under the QKD protocol was implemented correctly by the RX module under test.

— Step 6: Compare the sifted data from the RX module under test received through digital output 5 with the sifted data from the TX emulator through digital output 2. The expected relationships between elements of the sifted data depends upon the QKD protocol and the evaluator shall test whether the sifted data relates as expected. For example, in many discrete variable protocols, the two sets of sifted data include strongly correlated bit strings. In this case, the overlap between the main string of sifted bit values encoded by the TX emulator and the measured sifted bit string from the RX module under test provides a check of whether the measurements performed by the RX module under test were those intended. In such cases, overlap can be calculated as the number of bits in the main sifted bit strings divided by the total length of the main sifted bit strings. More detailed tests of the quality of the measurements performed on individual quantum states themselves are described in Clause 8.

6.2.3 Pass/fail criteria

The qualifying tests in steps 1, 4, and 5 shall be passed for both the TX module (see 6.2.2.1) and the RX module (see 6.2.2.2). Otherwise, the TOE fails the test.

In general, a set of thresholds shall be defined to appropriately compare the sifted data in step 6 for a particular protocol. For many protocols, the overlap between the TX and RX modules sifted bit strings and those of the corresponding RX and TX emulators, as defined in step 6 for each module type (see 6.2.2.1 and 6.2.2.2), is calculated over the accumulated data from n_{exe} sets of data. In this case, if both of the calculated overlaps are above a given threshold T_{overlap}, then the TOE passes the test. Otherwise, it fails the test.

Table 2 lists the threshold pertaining to the pass/fail decision of the EA for such cases.

Table 2 — Threshold for the pass/fail decision of the EA

No.	Threshold notation	Meaning of the threshold
1	T_{overlap}	The overlap between the main sifted data from the RX and TX modules corresponds to an agreement between the quantum states encoded and the results measured from the quantum states, when calculated for the accumulated data from n_{exe} sets of data.

In some protocols, detailed reconciliation procedures are required before strong correlations are revealed in the sifted data. Where step 6 of the above test procedures would not provide suitable assurance of the correctness of the quantum state encoding and measurement, alternative tests referring to 6.3 may be considered.

6.3 EA to test other post-processing procedures

6.3.1 General aspects

a) Objective of the evaluation activity

This EA intends to examine the correctness of the implementation of other post-processing functions subsequent to any sifting that is part of the QKD protocol. Sifting is a post-processing procedure but is evaluated under 6.2.

b) Required inputs

Besides the relevant documentation listed in the general input requirement, it is required to adapt the TOE to output a set of additional digital data to perform the test. A set of additional digital data shall provide data corresponding to the entire QKD session duration to test post-processing procedures performed on the entire block of data from a QKD session. It is sufficient for the QKD modules to output the additional digital data retrospectively. Data before sifting is not required to be output for this EA. Tests may be repeated where necessary to reduce statistical uncertainty in the results.

In addition, a sufficiently long common QKD authentication key shall be shared initially between the QKD module under test and the emulator.

The QKD module under test may be adapted such that the pre-shared QKD authentication key is reused for each QKD session in the test. This can reduce the length of the pre-shared QKD authentication key required to one that is sufficient to run any single QKD session. It is also possible for each QKD session in the test to consume a new section of the pre-shared key. In this case, the key shall be long enough for the entire test in this case.

c) Required tool types and setup

If the module under test is a QKD transmitter, an RX emulator with known characteristics is required. Likewise, if the module under test is a QKD receiver, a TX emulator with known characteristics is required. An emulator is defined as a tool with a known and trusted implementation of the expected functionality, which allows analysis of the TX (or the RX) module under test.

To conduct this EA, the evaluator shall have an emulator in advance. The emulator can be prepared by the evaluator themselves or can be implemented and then provided by the QKD manufacturer or the industrial community for evaluation. Either way, the emulator should be generally recognized by the evaluation authority.

A schematic of a common setup for testing the post-processing functionality of the TX module under test is shown in Figure 4. Post-processing may be structured differently from this example and is not required to be performed in the order shown.

The test is conducted on complete QKD modules adapted to provide the necessary additional digital data. In this EA, the raw data input to the error correction component is derived from the output of any sifting procedure in post-processing procedures (as evaluated in 6.2). More explanation for the setup is given in the rationale [d)] of this EA. Accordingly, the setup for testing other post-processing functionality subsequent to any sifting procedure of the RX module is quite similar and not detailed in this schematic.

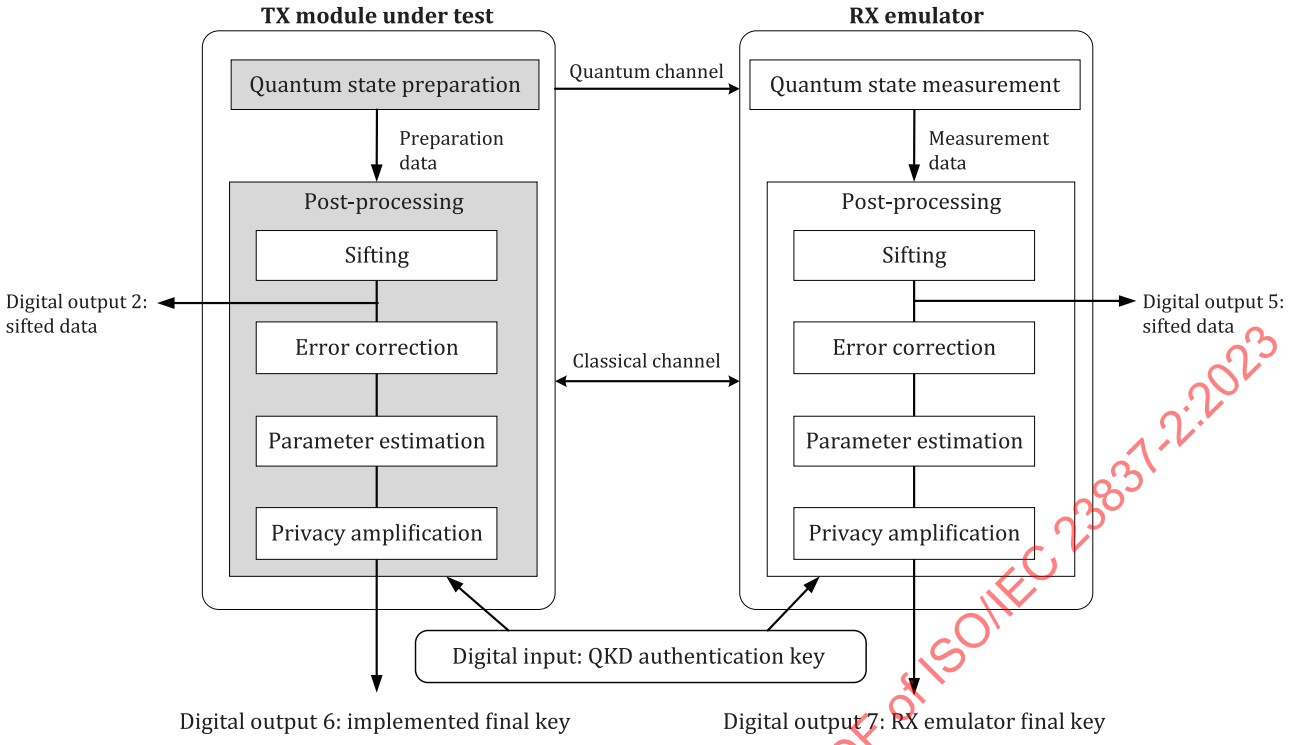


Figure 4 — Schematic of the setup for testing the post-processing functionality of a TX module

The sifting step is not required in some protocols, such as no switching CV QKD protocols. In this case, the output of quantum state preparation/measurement is used as the source for digital output 2 and digital output 5, respectively (see Figure 4).

In some cases, the post-processing procedures of a QKD protocol cannot be clearly separated and may be merged or run in parallel etc. Typically, parameter estimation begins earlier than shown and informs some parameters to error correction, but it also can use data from error correction.

d) Rationale

Since the QKD modules under test are operated as complete modules in the EA, the starting digital outputs for evaluating the subsequent post-processing components are derived from the output of the sifting procedure. An input parameter n_{exe} for this EA sets how many QKD sessions are required to be evaluated to ensure the test is statistically significant and shall be assigned before conducting the EA.

e) Dependencies

This EA shall be done after the quantum state transmission and sifting of post-processing procedures have been validated by passing the EA described in 6.2.

6.3.2 Test procedure

— Step 1: Prepare the environment for the test and connect the TX module under test and the RX emulator as required to perform the QKD protocol(s) to be evaluated. The initial step is to configure the TX module under test as the protocol requires.

— Step 2: Run a QKD session to generate final keys in the TX module under test and the RX emulator. The output of the TX module under test is recorded from digital output 6 and the input to the other post-processing procedures under test subsequent to the sifting procedure is recorded from digital output 2. The RX emulator final key is recorded as digital output 7 and the input to the post-processing procedures subsequent to the sifting procedure in the RX emulator is recorded from digital output 5.

NOTE The digital outputs 2, 5, 6, and 7 are shown in Figure 4.

— Step 3: Run step 1 to step 2 until n_{exe} QKD sessions have been completed and the results recorded, and ensure all the possible protocol configurations have been covered during the test. Then run step 4 to step 8 below.

— Step 4: For each QKD session, perform the full post-processing procedure on the sifted data recorded from the TX module under test and the RX emulator independently from the TOE to generate a fully emulated final key. This can differ from the key from step 2 since entropy is introduced when the post-processing procedures is repeated independently.

— Step 5: For each QKD session, test whether the TX module under test in step 2 delivered a final key whenever the RX emulator delivered a final key, or whether both the TX module under test and the RX emulator aborted the session and delivered no final key.

— Step 6: For each QKD session, compare the length of the final key from the TX module under test with the length of the fully emulated final key from step 4 to check that parameter estimation resulted in an appropriate amount of privacy amplification. Test that the final keys from the TX module under test are not longer than the final keys from step 4 on average by a statistically significant amount.

— Step 7: Count the number of overlapping bits in all the final keys from step 2 where the implemented final key bit from the TX module matches the RX emulator final key bit. Calculate the overlapping fraction by dividing this by the total number of bits in all the final keys from the TX module.

— Step 8: Repeat steps 1 to 8 similarly but with the TX emulator connected to the RX module under test. Then end the test.

6.3.3 Pass/fail criteria

The qualifying tests in steps 5 and 6 and the repeat of these steps with the TX emulator and the RX module under test as in step 8 shall be passed. Otherwise, the TOE fails the test.

If the overlapping fraction calculated in step 7 and the repeat of this step with the TX emulator and the RX module under test as in step 8 are both above a given threshold T_{PP} for post-processing, the test is passed. Otherwise, it fails. Table 3 lists the threshold pertaining to the pass/fail decision of the EA.

Table 3 — Threshold for the pass/fail decision of the EA

No.	Threshold notation	Meaning of the threshold
1	T_{PP}	The required minimum probability that the post-processing outputs or responses of the QKD module under test and the emulator are identical. The threshold is common to the paired QKD transmitter and QKD receiver modules.

NOTE The value of T_{PP} can be set to be 1, which means that if the final keys are not identical the test fails.

6.4 EA to test parameter adjustment procedure(s)

6.4.1 General aspects

a) Objective of the evaluation activity

This EA intends to validate the correctness of the TOE in implementing the SFR elements on parameter adjustment (i.e. FTP_QKD.1.6, FTP_QKD.1.7, and FTP_QKD.1.8). Specifically, it intends to examine:

1) Can the TOE initiate the relevant parameter adjustment procedure(s) if trigger events occur during a QKD session?

2) Can the TOE preserve a secure state when parameter adjustment procedure(s) are triggered and refuse to run any QKD session(s) until the parameter adjustment procedure(s) terminates, unless the restrictions on execution allow it to run QKD sessions simultaneously?

3) Can the TOE indicate the status of any parameter adjustment procedure(s)?

NOTE This EA does not intend to examine whether the parameter adjustment procedure(s) can really realign system parameters or not. This is mainly because the set of system parameters related to parameter adjustment procedure(s) are various and depend on the specific implementation of QKD modules. Therefore, it is difficult for this document to specify a general testing method of it. Further, the function of parameter adjustment procedure(s) is usually the content of performance testing of QKD modules; the validity of parameter adjustments is therefore omitted from the scope of security evaluation specification of this document.

b) Required inputs

The developer shall provide an entire TOE, including the two QKD modules under test. In addition, the TOE shall be prepared (or adapted) to allow the evaluator to trigger the parameter adjustment procedure(s), request to run QKD sessions, and observe the status indication of parameter adjustment.

c) Required tool types and setup

The two QKD modules under test are connected normally (such that they can run QKD sessions as in the normal state), as shown in Figure 5 for the example of a PM-QKD protocol but the EA is not limited to such protocols.

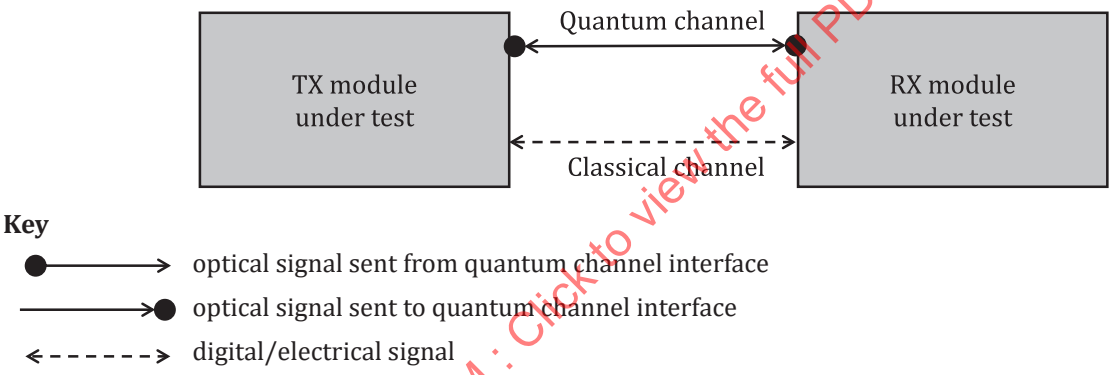


Figure 5 — Schematic of the setup for testing the parameter adjustment procedure(s)

d) Rationale

Generally, the parameter adjustment procedure(s) of QKD modules can be manually triggered by the administrator or automatically triggered by accidental failure events during the execution of the TOE. The actual trigger conditions are defined by the PP/ST in SFR element FTP_QKD.1.6 as shown in ISO/IEC 23837-1:2023, 9.3.2. For general purposes, this EA does not describe the specific trigger methods, but just assumes the evaluator can apply them to trigger the parameter adjustment procedure(s) during the execution of the TOE, though for some implementation strategies of the TOE, it should be adapted to provide this support.

Then, by checking the indication or status information of the TOE, the evaluator can examine whether the parameter adjustment procedure(s) of the QKD system is triggered or not. The indication method is specified by the PP or ST of the TOE in FTP_QKD.1.8, as shown in ISO/IEC 23837-1:2023, 9.3.2.

To examine whether the TOE refuses to run any QKD session before the end of any parameter adjustment procedure(s) that is not allowed to run simultaneously with QKD session(s), the evaluator asks the TOE to run QKD sessions during the procedure and checks the reaction of the TOE. For general purposes, this EA does not describe the methods of requesting the TOE to run QKD sessions, but assumes the

QKD modules under test can support the intention of the evaluator (which generally can be achieved by adapting the TOE somehow).

e) Dependencies

The EAs related to parameter adjustment procedure(s) are specified in two places in this document. In detail, the EA for examining the correct implementation of parameter adjustment procedure(s) is presented in 6.4, while the EA for examining the effectiveness of the IT-related controls to resist known attacks against parameter adjustment procedure(s) are presented in 9.2. The EA specified in 6.4 should be conducted before the EA in 9.2, and the EAs specified in 6.2 and 6.3 should be conducted before the EA in 6.4.

6.4.2 Test procedure

— Step 1: Run the TOE to perform QKD sessions.

— Step 2: For each trigger method assigned in the SFR element of FTP_QKD.1.6, apply it to trigger the parameter adjustment procedure(s), and do the following test until all cases have been tested:

  a) Observe the status changes of the TOE in order to validate whether the TOE can initiate the parameter adjustment procedure(s), and whether the TOE stops the on-going QKD session where the parameter adjustment procedure is not allowed to run simultaneously with QKD session(s) and indicates to the operator about the situation appropriately.

  b) During the parameter adjustment procedure(s), request that the TOE run a QKD session and examine whether the TOE refuses to execute it.

  c) When the parameter adjustment procedure(s) is finished, examine whether the TOE can run QKD sessions normally.

6.4.3 Pass/fail criteria

The test is passed if, for each trigger method assigned in the SFR element of FTP_QKD.1.6, the following conditions are satisfied together. Otherwise, the test has failed.

a) Each trigger method is effective in triggering the parameter adjustment procedure(s).

b) Before commencing a parameter adjustment procedure that is not allowed to run simultaneously with QKD session(s), the on-going QKD session is terminated and the relevant keying material generated during the relevant sessions is handled appropriately.

c) The TOE indicates the status of parameter adjustment procedure(s) in an appropriate way as defined in the SFR element FTP_QKD.1.8 and refuses to execute QKD sessions during the parameter adjustment procedure(s) that are not allowed to run simultaneously with QKD session(s).

d) When the parameter adjustment procedure(s) terminates successfully, QKD sessions can be executed as in the normal state.

There is no threshold pertaining to the pass/fail decision defined in the EA.

7 EAs for evaluating quantum optical components in the transmitter module

7.1 General

The EAs for the security evaluation of quantum optical components in TX modules are listed in Table 4. These EAs address potential flaws in quantum optical components of QKD modules that, if present, can otherwise compromise the security functions realizing the two security requirements FPT_EMS.1/Quantum and FPT_PHP.3. These flaws are known security-related issues of (or attacks against) TX modules that have been published and peer reviewed in academic literature. Although not all types of attacks have been demonstrated to date, at least a strategy for each type of attack has been reported.

Table 4 — EAs for quantum optical components in a TX module

Evaluation activity	Description	SFRs correspondence	Subclause index	Applicable protocols
Test the photon-number distribution of optical pulses	Test if emissions are consistent with the photon number distribution(s) of the optical pulses that are expected to be emitted by the TX module under test.	FPT_EMS.1/Quantum	7.2	DV-PM-QKD; DV-MDI-QKD; CV-PM-QKD; CV-MDI-QKD
Test the mean photon number and stability of optical pulses	Test if the mean photon number of the optical pulses generated in the TX module under test, as well as its stability in time are consistent with the requirements of the implemented QKD protocol.	FPT_EMS.1/Quantum	7.3	DV-PM-QKD; DV-MDI-QKD; CV-PM-QKD; CV-MDI-QKD
Test the independence of the intensities of optical pulses	Test if the intensities of the emitted pulses for each intended intensity are independent of the underlying intensity modulation pattern.	FPT_EMS.1/Quantum	7.4	DV-PM-QKD; DV-MDI-QKD; CV-PM-QKD; CV-MDI-QKD
Test the accuracy of state encoding	Test if the quantum states emitted by the TX module under test are encoded sufficiently accurately to match those required by the implemented QKD protocol.	FPT_EMS.1/Quantum	7.5	DV-PM-QKD; DV-MDI-QKD
Test the indistinguishability of encoded states	Test if the different quantum states encoded in a same degree of freedom can be distinguished from the perspective of non-encoding degrees of freedom.	FPT_EMS.1/Quantum	7.6	DV-PM-QKD; DV-MDI-QKD; CV-PM-QKD; CV-MDI-QKD
Test the uniform distribution of the global phase of optical pulses	Test if the global phase of optical pulses is randomly distributed, as required by the implemented QKD protocol.	FPT_EMS.1/Quantum	7.7	DV-PM-QKD; DV-MDI-QKD;
Test the degree of optical isolation of the TX module	Test if the isolation ability provided by the TX module under test suffices to prevent the light injected from the quantum channel to the module.	FPT_PHP.3	7.8	DV-PM-QKD; DV-MDI-QKD; CV-PM-QKD; CV-MDI-QKD
Test the sensitivity of the injected light monitor in the TX module	Test if the injected light monitor deployed to detect light injected by an adversary through the quantum channel interface works properly. Characterize its sensitivity under continuous-wave emission and high-frequency/narrow-width optical pulses.	FPT_PHP.3	7.9	DV-PM-QKD; DV-MDI-QKD; CV-PM-QKD; CV-MDI-QKD
Test the robustness of the TX module against laser injection	Test the robustness of the TX module under test against laser light injected through the quantum channel interface.	FPT_PHP.3	7.10	DV-PM-QKD; DV-MDI-QKD; CV-PM-QKD; CV-MDI-QKD

a) General description of inputs

The TX module should be operated under conditions that are as close to normal operating conditions as possible, which means the security test procedures should be conducted on the TX module as a whole, without requiring additional interfaces, channels, or outputs other than those already present on the

TX module. Its objective is to reflect the security status of actual QKD modules under the conditions they face in operation.

Some of the EAs mentioned in Clause 7 require the TX module under test to be configured to emit pulses equivalent to those in the raw data generation stage. Here "equivalent" means:

— Pulses are transmitted with intensities used in the raw data generation stage.

— Pulses are encoded with a random sequence used in the raw data generation stage.

— For QKD protocols in which the TX module under test is required to emit optical pulses of more than one intensity, pulses are modulated to a sequence of intensity states used in the raw data generation stage.

In order to conduct the EM effectively, EAs may allow more modifications to the TOE, for example:

— In a limited number of instances, if the information gained from measuring the whole system is insufficient, individual components or sub-assemblies of QKD modules may be tested (see 7.8).

— Where a TX module supports reducing its internal attenuation in a test mode, the attenuation inside the TX module may be reduced such that the optical pulses can be emitted at a higher average intensity level than in the raw data generation stage, in order to relax the sensitivity requirements of test tools and/or to reduce the duration of measurements (see 7.4, 7.6, 7.7, and 7.10).

— Digital output indicating the order of states emitted from the TX module may be enabled where needed to analyse the measurement result of those states (see 7.2 to 7.7 and 7.10).

— The TX module may be configured to emit an appropriate repeating pattern of states that is known to the evaluator. Such repeating patterns should typically be representative of patterns used in operation so that results are representative of the TX module in operation.

— A specially configured TX module may be used, e.g. to ignore repeated failures without transitioning to a failure state for the duration of an EA.

Where an EA requires modifying the operation of a TX module, the modification should be specified in the description of required inputs of the EA. It is implicitly assumed that the modification is removed or disabled after testing.

b) General description of test tools and setup

When performing the EAs in 7.2 to 7.10, the evaluator shall set up the test following best engineering practice and considering the specific characteristics of the instruments used. For example, SPDs are selected with a suitable clock rate, dead time, and noise level to perform the measurement on the TX module under test. The QKD protocol and design of the QKD modules can influence the detectors that are suitable for testing a given TX module. When planning the tests and analysing the results, the details of the performance of the detectors used should be considered, including dark counts, after pulses and time jitter that can occur during measurements. Any corrections made to account for the non-ideal behaviour of instruments shall be reasonable. Care shall be taken to ensure that corrections are performed in a manner that does not compromise the objectives of the EAs.

For those EAs that require the TX module to emit pulses equivalent to those in the raw data generation stage, the TX module can often do this only when connected to a compatible RX module. In such cases, it is appropriate to introduce an RX emulator to provide the signals expected by the TX module under test to enable it to be operated as required. Specifically:

— The RX emulator can supply trigger signals to the TX module under test and other test tools, or receive trigger signals from other tools.

— The required timing signals can be derived from signals present in the optical link between the TX module under test and the RX emulator.

— The optimal way to combine or split communications between a TX module under test and an RX emulator and signals to/from other tools depends upon the EA and details of the TX module under test. Optical couplers or wavelength multiplexing devices are usually suitable.

In some cases, an RX module under test can be used as an RX emulator.

7.2 EA to test the photon-number distribution of optical pulses

7.2.1 General aspects

a) Objective of the evaluation activity

This EA intends to test whether emissions are consistent with the photon number distribution(s) of the optical pulses that are expected to be emitted by the TX module under test.

b) Required inputs

The developer shall provide the TX module under test, which is configured to emit pulses equivalent to those emitted in the raw data generation stage. The TX module under test shall allow the evaluator to access time tagged digital data containing the intensity modulation pattern used by the TX module during the test.

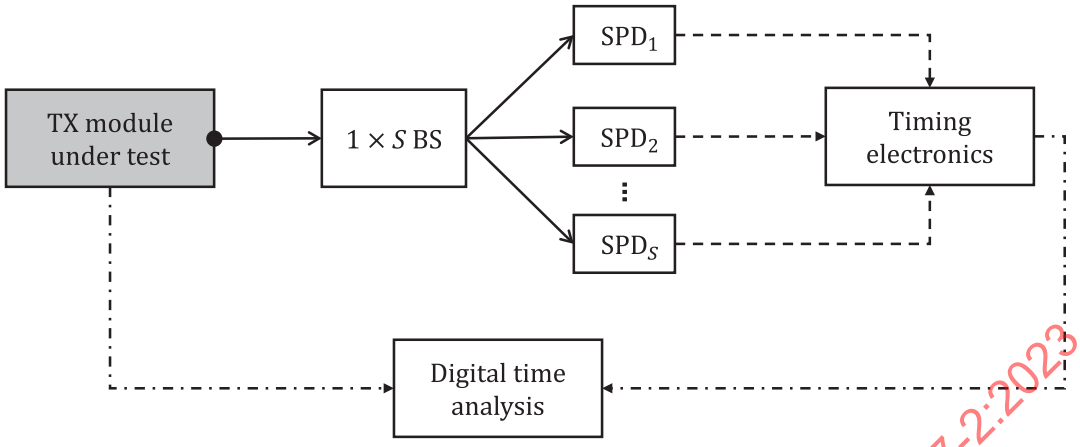
c) Required tool types and setup

The evaluator shall prepare a $1 \times S$ beam splitter (BS) or equivalently a cascade of BS to realize the same $1 \times S$ splitting function. The input of the BS is connected to the quantum channel, which is connected on the other end to the quantum channel interface of the TX module under test. The output ports of the BS are connected to S single-photon detectors (SPD_1, ..., SPD_S), whose outputs are connected to timing electronics capable of counting coincidences.

In this EA, a k-coincidence is taken to be the occurrence of a detection event in k of the SPDs at times that are consistent with the arrival of a particular quantum state from the TX module at each SPD after considering jitter and latency. For gated SPDs, this may be taken as the occurrence of a detection event in k of the SPDs in detector gates that are consistent with the arrival of a particular quantum state from the TX module at each SPD.

The output of the timing electronics is used to calculate the k-th order correlation function $g^{(k)}(t)$ at zero delay ($t = 0$), where $k \in \{2,3,...,S\}$ is an integer representing the order of the correlation function, which is upper bounded by S and decided by the evaluator, and t is a time delay. The evaluator shall also prepare timing electronics to time tag the output of SPDs and a tool for the digital time analysis of the digital data coming from the TX module under test and the timing electronics.

The schematic of the setup for performing the EA is a generalized Hanbury-Brown-Twiss interferometer, as shown in Figure 6.



Key

optical signal sent from quantum channel interface
optical signal
digital/electrical signal
digital data

Figure 6 — Schematic of the setup for testing the photon-number distribution of optical pulses

d) Rationale

The photon number distribution(s), $P(m)$, of the optical pulses represents the probabilities that a pulse contains m photons. The outcome of the test shall indicate whether the $P(m)$ measured from the TX module under test follows the theoretical distribution assumed in the QKD protocol. However, rather than testing $P(m)$ directly, the evaluator shall test correlation functions $g^{(k)}(t=0)$, with k an integer larger than 1. There is a known relation between the photon number distribution, $P(m)$, and the correlation functions $g^{(k)}(0)$ at zero delay, which is denoted by $g^{(k)}$ for simplicity in this EA.

For the case of k = 2, for example, the correlation function can be expressed as Formula (1)

$$g^{(2)} = \sum_m P(m)[m(m-1)] \Big/ \mu^2 \tag{1}$$

where

μ is the mean number of photons in an optical pulse, which is measured in another evaluation activity (see 7.3);

m is the photon number of an optical pulse;

$g^{(2)}$ is the second order correlation function at zero delay.

Thus, the correlation functions $g^{(k)}$ indirectly indicate whether the emitted photon number distribution follows the theoretical distribution expected under the QKD protocol. The SPDs produce "clicks" recorded by the timing electronics together with their time tags. Simultaneous clicks from SPD_1 and SPD_2 are used in determining $g^{(2)}$. Simultaneous clicks from SPD_1, SPD_2, and SPD_3 are used in determining $g^{(3)}$. In general, the simultaneous clicks from SPDs from 1 to k are used in determining $g^{(k)}$. If the deviations between the measured $g^{(k)}$ and the theoretical values are within certain thresholds, it means the photon number distribution follows the theoretical distribution within a certain tolerance and this EA's test has passed.

If the TX module under test is required to emit more than one intensity of optical pulse under the QKD protocol, the evaluator can use the time tags registered by the timing electronics to correlate the clicks of the detectors with the intensities emitted by the TX module under test. This allows the evaluator to infer the $g^{(k)}$ functions for each of the intensities set by the TX module under test while operating a particular QKD protocol.

Clause 12 permits this EA to be replaced with an alternative EA using a different measurement method to estimate the photon number distribution $P(m)$. For example, measurements using a photon-number-resolving detector would be a possible basis for an alternative EA.

7.2.2 Test procedure

The test procedure below is described for the case where the QKD protocol requires the TX module to emit optical pulses with a single intensity. If more than one intensity is emitted, the evaluator shall repeat the analysis in steps 4 to 7 of the test procedure described below for each intensity, considering only the relevant optical pulses in each analysis.

— Step 1: Turn on the TX module under test and configure it to emit pulses equivalent to those in the raw data generation stage.

— Step 2: Where gated SPDs are used, adjust the timing of signals used to trigger the SPDs such that the optical pulses from the TX module under test arrive during the gates of the SPDs.

— Step 3: Record the number of optical pulses, N_{pulse}, emitted for an acquisition time that is long enough to obtain sufficient S-coincidence counts in the SPDs from 1 to S to determine the S–1 deviations in Step 7 to the required precision.

— Step 4: Record the number of single clicks from SPDs in Figure 6 and denote by N_1, N_2, ..., N_S, and record the number of k-coincidence counts from the first k SPDs in Figure 6 and denote by $N_{\text{c}}^{(k)}$ with $k \in \{2,3,...,S\}$.

NOTE 1 In most cases, measuring $g^{(k)}$ up to $k = 4$ is sufficient to determine the photon number distribution of the TX module tightly.

NOTE 2 The k-coincidence counts also can be estimated from an appropriate combination of detection outcomes of the SPDs. For example, for $S = 4$, it is possible to estimate $N_{\text{c}}^{(2)}$ from the detection outcomes of detector groups {12, 13, 14, 23, 24, 34}, $N_{\text{c}}^{(3)}$ from detector groups {123, 124, 134, 234} and $N_{\text{c}}^{(4)}$ from detector group {1234}.

— Step 5: Calculate the single count probability from the i-th SPD as $P_i = N_i / N_{\text{pulse}}$ and the coincidence count probability from the first k SPDs as $P_{\text{c}}^{(k)} = N_{\text{c}}^{(k)} / N_{\text{pulse}}$ with $k \in \{2,3,...,S\}$.

— Step 6: Calculate the measured value of the correlation functions up to the order S, as Formula (2):

$$g_{\text{M}}^{(k)} = \frac{P_{\text{c}}^{(k)}}{P_1 P_2 \cdots P_k} \tag{2}$$

where $k \in \{2,3,...,S\}$.

— Step 7: Calculate the deviations between the measured $g_{\text{M}}^{(k)}$ obtained in the previous step and the theoretical $g_{\text{T}}^{(k)}$ expected for the TX module under test, as Formula (3):

$$\Delta^{(k)} = \left| g_{\text{M}}^{(k)} - g_{\text{T}}^{(k)} \right| \tag{3}$$

where $k \in \{2,3,...,S\}$.

7.2.3 Pass/fail criteria

If the TX module under test is operating a QKD protocol that only requires the emission of optical pulses into the quantum channel of equal intensity, then if each measured $\Delta^{(k)}$ is smaller than the k-th threshold value $T_{\text{diffCor}(k)}$, the test has passed. Otherwise, the test has failed.

If a QKD protocol requires the TX module to emit more than one intensity of optical pulse into the quantum channel, the developer may optionally indicate a different $T_{\text{diffCor}(k)}$ for each intensity or may indicate that the same threshold applies to all intensities. Some QKD protocols require such TX modules to emit with a certain probability pulses of very small intensity, corresponding to an approximation to the "vacuum" state. For these special states, moderate deviations in the photon number statistics are typically not very significant in the overall security analysis and obtaining a statistically significant measure of $\Delta^{(k)}$ may not be practical. If each measured $\Delta^{(k)}$ calculated for each subset of optical pulses, corresponding to a different intensity in the QKD protocol other than any "vacuum" state, is smaller than the relevant k-th threshold value $T_{\text{diffCor}(k)}$ for that intensity, the test has passed. Otherwise, the test has failed.

Table 5 lists the threshold pertaining to the pass/fail decision of the EA.

Table 5 — Threshold for the pass/fail decision of the EA

No.	Threshold notation	Meaning of the threshold
1	$T_{\text{diffCor}(k)}$	The absolute value of the difference between the measured value and the theoretical value of the k-th order correlation function, for a fixed intensity of the pulses emitted by the TX module. Where a QKD protocol requires the TX module to emit pulses of more than one intensity different thresholds may optionally be indicated for different intensities.

7.3 EA to test the mean photon number and stability of optical pulses

7.3.1 General aspects

a) Objective of the evaluation activity

This EA intends to test the mean photon number of the optical pulses generated in the TX module under test, as well as its stability in time. The testing outcome indicates whether the mean photon number of the optical pulses falls consistently within the expected threshold limits.

b) Required inputs

The developer shall provide a TX module under test, which is configured to emit pulses equivalent to those emitted in the raw data generation stage. The TX module under test shall allow the evaluator to access time tagged digital data containing the intensity modulation pattern used by the TX module during the test.

c) Required tool types and setup

The evaluator shall prepare a calibrated optical detector that works below its saturation level and above its intrinsic noise level with known detection efficiency, η_{det}, which shall be connected to the quantum channel interface of the TX module under test via a calibrated link of known transmissivity, η. The detector shall be sensitive to the output of the TX module under test.

The evaluator shall also prepare timing electronics to time tag the output of the calibrated optical detector and a tool for the digital time analysis of the digital data coming from the TX module under test and the timing electronics.

NOTE A detector typically works best if it is well within its dynamic range, i.e. well below its saturation level and well above its intrinsic noise level. It is noted that for single photon detectors, the assumption that the intensity is proportional to the number of detection events counted is only reasonable under such conditions.

The schematic of the setup for performing the EA is shown in Figure 7.

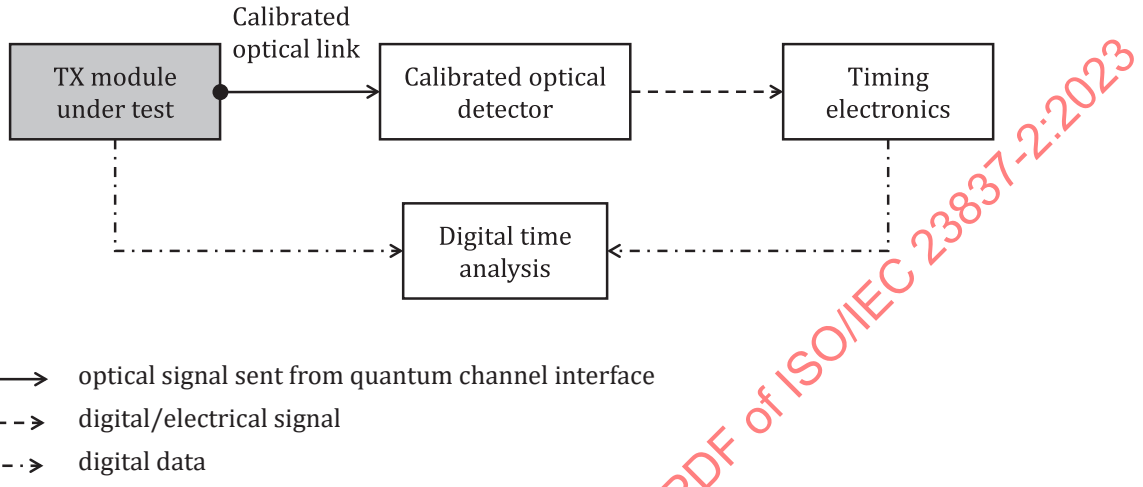


Figure 7 — Schematic of the setup for testing the mean photon number and stability of optical pulses

d) Rationale

This EA checks the mean photon number of the optical pulses generated and emitted by the TX module under test. It performs the measurement repeatedly over a period of time to assess the stability of the mean photon number. The TX module under test emits optical pulses with K intensity levels, where K is an integer number. The mean photon number is equivalent to knowing the intensity, where other information about the optical pulses, such as their wavelength and speed, is also known.

The calibrated optical detector may measure either the pulse energy or, for a single photon detector, whether or not a detection event was registered for each optical pulse. For an intensity k, the average pulse energy, E_k, is derived from summing the total energy, I_k, in each relevant pulse and dividing by the number of relevant pulses, N_k. Alternatively, the mean photon number, μ_k, is derived from counting the total number of relevant photon detection events, C_k, and dividing the number of relevant pulses, N_k.

The measurement is repeated M times and the average pulse energy or mean photon number for each measurement is checked against the threshold limit after correction for transmission loss and detector efficiency.

7.3.2 Test procedure

— Step 1: Turn on the TX module under test and configure it to emit pulses equivalent to those emitted in the raw data generation stage and connect it to the calibrated optical detector with detection efficiency, η_{det}, through a calibrated link of known transmission efficiency, η. If necessary, calibrated attenuation may be introduced before the calibrated optical detector to reduce the intensity to f times the intensity emitted by the TX module, such that the intensities incident on the detector are in the calibrated range over which the detector is designed to operate. If a gated calibrated detector is used, adjust the timing of the gates such that the optical pulses arrive during the gates of the detector and synchronize the output with the timing electronics if necessary.

— Step 2: Measure a stream of N_{pulse} optical pulses coming out of the TX module under test during the acquisition time with the calibrated optical detector. Use the timing electronics to record data to enable each result to be matched up with a specific pulse emitted by the TX module under test. Here, N_{pulse} is a parameter equivalent to the acquisition time that should be chosen to enable a sufficient number of pulses to be measured to give average pulse energies or mean photon numbers with errors that are sufficiently small, relative to the difference between the maximum and minimum threshold limits to enable the test to be performed reliably. Some QKD protocols require TX modules to emit pulses of very small intensity with a certain probability, corresponding to an approximation to the "vacuum" state. For these special states, the required acquisition time can be considered long enough if any background signals (such as dark counts) can be measured to the necessary precision.

— Step 3: Where necessary, align the digital strings from the calibrated detector with the pulse intensity pattern set by the TX module under test. For example, by using the digital data coming from the TX module under test and the time-tagged digital data coming from the timing electronics, the evaluator can cross-correlate the intensity modulation pattern coming from the TX module under test with the results measured by the calibrated optical detector. This allows the evaluator to know what intensity setting was set by the TX module under test for the pulse present for each measurement by the calibrated detector.

— Step 4: Group all the emitted optical pulses where the TX module under test set the same intensity level. This returns K data sets, S_k, each of length N_k, with $\sum_{k=1}^{K} N_k = N_{\text{pulse}}$, where the subscript k is the label value for the intensity set by the TX module.

— Step 5: If the calibrated detector is of the single photon type, sum up how many photon detection events, C_k, are present in each data set, S_k. By dividing the counts, C_k, by the length of the data set, N_k, the evaluator can determine the probability that a pulse where the TX module set intensity k resulted in a photon detection event in the calibrated detector, $P_k = C_k / N_k$. For a calibrated detector with photon number discrimination capabilities, this will represent the mean number of photons detected by the calibrated detector for each pulse where the TX module set intensity k.

For other types of calibrated detectors, sum up the total energy detected, I_k, in each data set S_k. By dividing the total detected energy, I_k, by the length of the data set, N_k, the evaluator can obtain the average energy detected by the calibrated detector for a pulse where the TX module set intensity k, $E_k = I_k / N_k$.

— Step 6: For each k, calculate the mean photon number using Formula (4):

$$\mu_k = P_k / (\eta_{\text{det}} \eta) \tag{4}$$

or Formula (5):

$$\mu_k = E_k \lambda / (\eta_{\text{det}} \eta h c) \tag{5}$$

where

λ is the wavelength of the optical pulses emitted by the TX module;

h is Planck constant;

c is the speed of the optical pulses travelling in the calibrated optical link.

If attenuation was introduced before the calibrated detector, the mean photon number shall be corrected as shown in Formula (6):

$$\mu_k = P_k / (\eta_{\text{det}} \eta f) \tag{6}$$

or Formula (7)

$$\mu_k = E_k \lambda / (\eta_{\text{det}} \eta f \hbar c). \tag{7}$$

— Step 7: Repeat the measurement M times, and for each measurement determine a set of K mean photon numbers (one set for each of the M measurements).

7.3.3 Pass/fail criteria

If each of the $K \times M$ measured mean photon numbers is within the range defined by the minimum acceptable mean photon number, $T_{\text{minMPN}(k)}$, and the maximum acceptable mean photon number, $T_{\text{maxMPN}(k)}$, the test has passed. Otherwise, it has failed.

Table 6 lists the thresholds pertaining to the pass/fail decision of the EA.

Table 6 — Thresholds for the pass/fail decision of the EA

No.	Threshold notation	Meaning of the threshold
1	$T_{\text{minMPN}(k)}$	The minimum acceptable mean photon number (this threshold may be zero). There is one such threshold for each intensity k that the TX module is required to emit under a QKD protocol.
2	$T_{\text{maxMPN}(k)}$	The maximum acceptable mean photon number output by the TX module. There is one such threshold for each intensity k that the TX module is required to emit under a QKD protocol.

7.4 EA to test the independence of the intensities of optical pulses

7.4.1 General aspects

a) Objective of the evaluation activity

This EA intends to test the common assumption in QKD protocols that the intensities of the emitted pulses for each intended intensity are independent of the underlying intensity modulation pattern. For that, the EA aims to characterize the potential intensity correlations of the optical pulses emitted by the TX module under test. The description of the EA is limited to adjacent optical pulses, but it can easily be generalized to any group of pulses emitted by the TX module under test.

This EA applies to QKD protocols that emit optical pulses with different intensities.

b) Required inputs

The developer shall provide a TX module under test, which is configured to emit pulses equivalent to those emitted in the raw data generation stage. The TX module under test shall allow the evaluator to access time tagged digital data containing the intensity modulation pattern used by the TX module during the test. The developer may optionally reduce the value of attenuation inside the TX module under test to emit pulses at a higher average intensity level than in the raw data generation stage.

c) Required tool types and setup

This EA adopts a setup similar to the EA in 7.3. The evaluator shall prepare an optical detector that works below its saturation level and above its intrinsic noise level but whose efficiency need not be calibrated. The optical detector shall be sensitive to the output of the TX module under test and shall be capable of resolving each pulse in time. The detector is connected to the quantum channel interface of the TX module under test.

The evaluator shall also prepare timing electronics to time tag the output of the optical detector and a tool for the digital time analysis of the digital data coming from the TX module under test and the timing electronics.

The schematic of the setup for performing the EA is shown in Figure 8.

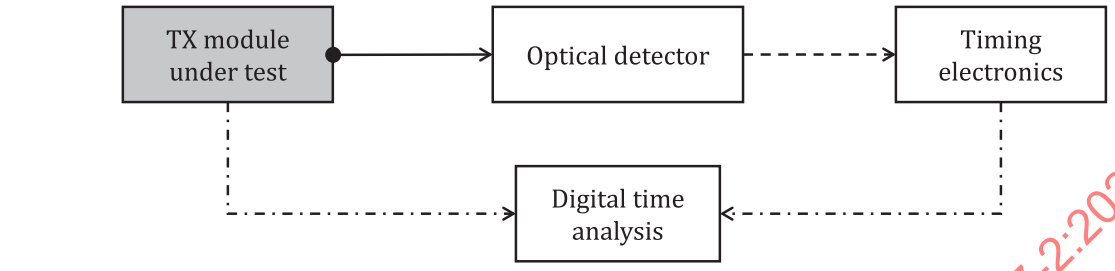


Figure 8 — Schematic of the setup for testing the independence of the intensities of optical pulses

d) Rationale

This EA intends to examine how the intensity of a given pulse is dependent on the intensity of the pulse that preceded it in the modulation pattern. During the test, the TX module under test emits optical pulses with K intensity levels, where K is a positive integer. Each pulse is measured by a detector, the results are grouped according to the intensity levels of the pulse and its preceded pulse in the modulation sequence. The average pulse energy or detection probability for each group is then calculated. The maximum difference between any of these averages for pulses with same intensity level are then calculated and compared against a specified threshold to give a verdict for this EA.

7.4.2 Test procedure

— Step 1: Turn on the TX module under test and configure it to emit pulses equivalent to those emitted in the raw data generation stage (apart from optionally their intensity if the internal attenuation is reduced during the measurement) and connect it to the optical detector. If a gated detector is used, adjust the timing of the gates such that the optical pulses arrive during the gates of the detector and synchronize the timing electronics with the emission times of the optical pulses.

— Step 2: Measure a stream of N_{pulse} optical pulses coming out of the TX module under test during the acquisition time with the optical detector, use the timing electronics to record data to enable each result to be matched up with a specific pulse emitted by the TX module. Here, N_{pulse} is a parameter equivalent to the acquisition time. It should be chosen to enable the sufficient number of pulses to be measured to give detection probabilities or average pulse energies with errors that are sufficiently small to calculate the resulting deviation in the absence of undesirable correlations.

— Step 3: Where necessary, align the digital strings coming from the calibrated detector with the pulse intensity pattern set by the TX module under test. For example, by using the digital data coming from the TX module under test and the time-tagged digital data coming from the timing electronics, the evaluator can cross-correlate the intensity modulation pattern coming from the TX module under test with the counts measured by the optical detector. This allows the evaluator to know what intensity setting was set by the TX module under test for the pulse present for each measurement by the optical detector.

— Step 4: Group all the emitted optical pulses that belong to the same intensity level, μ_k, and that were preceded by an optical pulse of intensity level, μ_j, where $k, j \in \{1,2,...,K\}$. This returns K^2 strings, $S_{k|j}$, each of length $N_{k|j}$, each containing only events from pulses prepared with intensity μ_k that were preceded by a pulse prepared with intensity μ_j.

NOTE This step can be generalized to any desired condition for the intensity correlation test, for instance, to three or more consecutive optical pulses or any other conceivable intensity modulation pattern. It is not expected to have two consecutive detections in the optical detector to record an entry in a string $S_{k|j}$. The result of each measurement performed is recorded in only one of the strings.

— Step 5: If the optical detector is of the single photon type, sum up how many photon detection events, $C_{k|j}$, is present in each string $S_{k|j}$. By dividing the counts $C_{k|j}$ by the length of the string $N_{k|j}$, extract the detection probability of a count in that string, $P_{k|j} = C_{k|j} / N_{k|j}$. For an optical detector with photon number discrimination capabilities, this will represent the mean number of photons detected for each pulse where the TX module set intensity *k*.

For other types of optical detectors, sum up the total energy detected, $I_{k|j}$, in each string $S_{k|j}$. By dividing the total detected energy, $I_{k|j}$, by the length of the string $N_{k|j}$, the evaluator can extract the average pulse energy, $E_{k|j} = I_{k|j} / N_{k|j}$.

— Step 6: For all $k, j, i \in \{1,2,...,K\}$, calculate the differences using Formula (8):

$$\delta_{k,j,i} = \left| P_{k|j} - P_{k|i} \right| \tag{8}$$

or Formula (9):

$$\delta_{k,j,i} = \left| E_{k|j} - E_{k|i} \right| \tag{9}$$

where $j \neq i$.

7.4.3 Pass/fail criteria

If $\delta_{k,j,i}$ for all *k*, *j*, *i*, where *j* is not equal to *i*, is smaller than the designed threshold, $T_{\text{diffAvInten}}$, on the maximum difference, the test has passed. Otherwise, it has failed.

Table 7 lists the threshold pertaining to the pass/fail decision of the EA.

Table 7 — Threshold for the pass/fail decision of the EA

No.	Threshold notation	Meaning of the threshold
1	$T_{\text{diffAvInten}}$	Maximum difference between the average intensities of optical pulses prepared with the same intensity setting that were preceded by an optical pulse prepared with any specific intensity setting and those preceded by an optical pulse prepared with any other specific intensity setting.

7.5 EA to test the accuracy of state encoding

7.5.1 General aspects

a) Objective of the evaluation activity

This EA intends to test whether the quantum states emitted by the TX module under test are encoded sufficiently accurately to match those required by the implemented QKD protocol.

b) Required inputs

The developer shall provide the TX module under test, which is configured to emit pulses equivalent to those emitted in the raw data generation stage. The TX module under test shall allow the evaluator to access time tagged digital data containing the intensities and states encoded by the TX module during the test.

c) Required tool types and setup

The evaluator shall prepare a quantum state analyser connected to the quantum channel interface of the TX module under test. The quantum state analyser can, for example, be either specified as:

— a polarization analyser for a polarization encoding system;

— a phase interferometer for a phase encoding system;

— a time-phase interferometer for a time-bin encoding system.

In practice, the quantum state analyser should be instantiated according to the concrete encoding method adopted by the TOE. The quantum state analyser shall be chosen to have sufficient sensitivity to measure the output of the TX module under test.

The evaluator shall also prepare timing electronics to time tag the output of the calibrated optical detector and a tool for the digital time analysis of the digital data coming from the TX module under test and the timing electronics.

The schematic of the setup for performing this EA is shown in Figure 9.

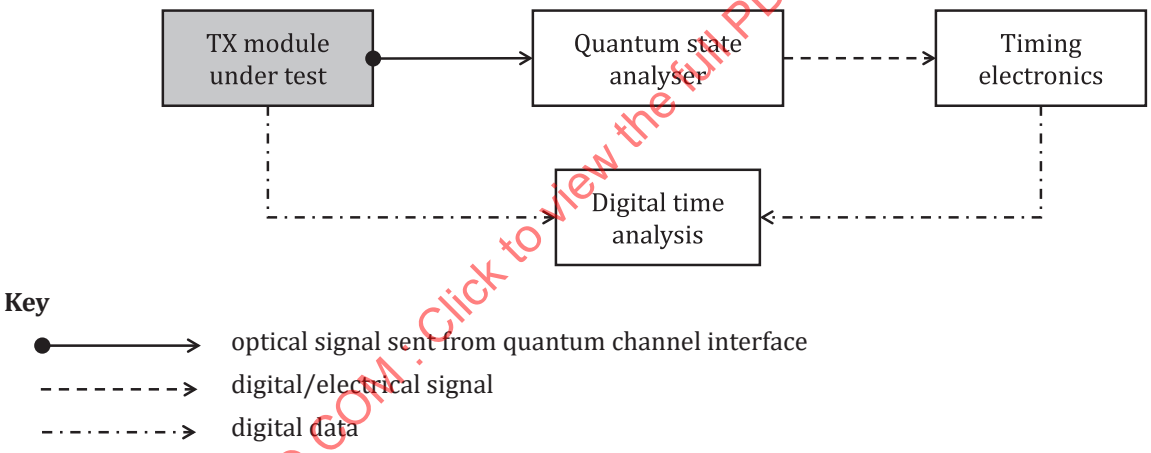


Figure 9 — Schematic of the setup for testing the accuracy of state encoding

d) Rationale

This EA tests the fidelity between the practical quantum states sent by the TX module under test and the ideal ones required by the QKD protocol. The evaluator analyses density matrices of the encoded states emitted by the TX module under test with a quantum state analyser and calculates the fidelities between the measured states and the ideal ones. The minimum fidelity is used to give a verdict against a specified threshold.

7.5.2 Test procedure

— Step 1: Turn on the TX module under test and configure it to emit pulses equivalent to those emitted in the raw data generation stage. All states shall be encoded and emitted according to the requirements of the QKD protocol.

— Step 2: Measure all the emitted states during an acquisition time with the quantum state analyser and use the timing electronics to time tag each of the outcomes with a progressive period number.

— Step 3: Where necessary, align the digital strings coming from the quantum state analyser with the pattern of encoded states set by the TX module under test. For example, by using the digital data coming from the TX module under test and the time-tagged digital data coming from the timing electronics, the evaluator can cross-correlate the results measured by the quantum state analyser with the pattern of encoded states coming from the TX module under test. This allows the evaluator to know what state was set by the TX module for the pulse present for each measurement by the quantum state analyser.

— Step 4: Group all the results according to the state the TX module encoded. Construct the density matrices of specific encoded states emitted by the TX module under test, denoting them by ρ_i where each *i* represents a specific encoded quantum state.

  Various techniques, such as maximum likelihood estimates, may be used to estimate physical density matrices from measured data. Density matrices may alternatively be estimated with models for particular types of encoding errors. An evaluator can effectively target the most likely errors in this manner.

— Step 5: Calculate the fidelity between the measured density matrices, ρ_i, and the ideal density matrices assumed in the QKD protocol, ρ_i^{T}, using Formula (10):

$$F_i = \left(\mathrm{tr}[\sqrt{\rho_i^{1/2}\rho_i^{\mathrm{T}}\rho_i^{1/2}}]\right)^2 \tag{10}$$

  where $\mathrm{tr}[\cdot]$ is the trace of a matrix.

  Alternatively, one may also use the square root fidelity $\sqrt{F_i} = \mathrm{tr}[\sqrt{\rho_i^{1/2}\rho_i^{\mathrm{T}}\rho_i^{1/2}}]$ to measure the accuracy of the state encoding here.

— Step 6: Calculate the minimum fidelity over all the encoded states using Formula (11):

$$F = \min_i\{F_i\} \tag{11}$$

  where $\min\{\cdot\}$ is the minimum value in a set.

  Random or targeted sampling of states may be adopted to estimate *F* rather than deriving it by estimating fidelity for each possible encoded state. Some protocols, such as CV-QKD, can use a large number of states.

7.5.3 Pass/fail criteria

If the minimum measured fidelity *F* is larger than the designed threshold T_{minFid}, the test has passed. Otherwise, it has failed.

Table 8 lists the threshold pertaining to the pass/fail decision of the EA.

Table 8 — Threshold for the pass/fail decision of the EA

No.	Threshold notation	Meaning of the threshold
1	T_{minFid}	The minimum tolerable fidelity between the density matrix of the encoded quantum state and the ideal encoded state is required by the implemented QKD protocol.

7.6 EA to test the indistinguishability of encoded states

7.6.1 General aspects

a) Objective of the evaluation activity

This EA intends to test if the different quantum states encoded in the same degree of freedom can be distinguished from the viewpoint of non-encoding degrees of freedom. The non-encoding degrees of freedom considered in this EA include the wavelength, the polarization, and the arrival time. Where a QKD protocol encodes in one of these three degrees of freedom, this degree of freedom shall be excluded from measurement under this EA. The test outcome indicates whether the TX module under test is prone to side channel attacks in non-encoding degrees of freedom.

b) Required inputs

The developer shall provide the TX module under test, which is configured to emit pulses equivalent to those in the raw data generation stage. The TX module under test shall allow the evaluator to access time tagged digital data containing the intensities and states encoded by the TX module during the test. The developer may optionally reduce the value of attenuation inside the TX module under test to emit pulses at a higher average intensity level than in the raw data generation stage.

c) Required tool types and setup

The evaluator shall prepare an optical detector, a spectrum analyser working in an appropriate wavelength range, and a polarization analyser. All these measurement devices shall be sensitive to the output of the TX module under test and be connected to the quantum channel interface of the TX module under test via beam splitters (BS).

The evaluator shall also prepare timing electronics to time tag the output of these devices and a tool for the digital time analysis of the digital data coming from the TX module under test and the timing electronics.

The schematic of the setup for this EA is shown in Figure 10.

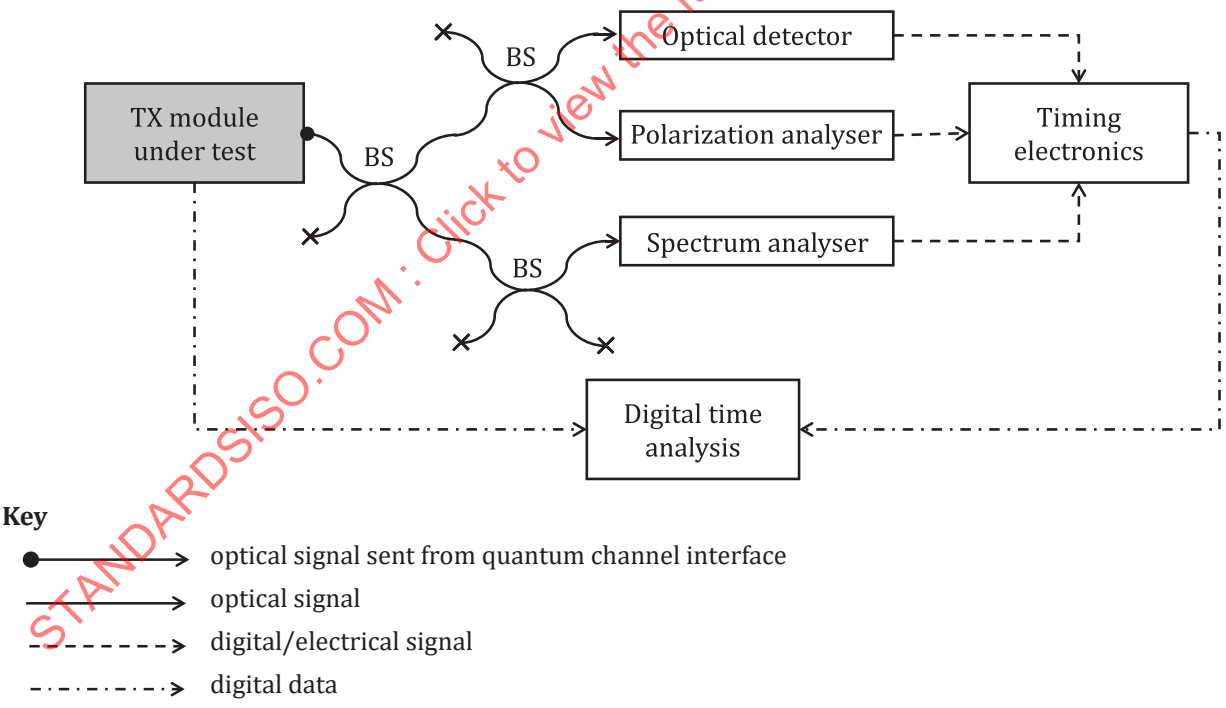


Figure 10 — Schematic of the setup for testing the indistinguishability of encoded states

d) Rationale

This EA characterizes the differences of probability distribution/trace distance over all encoded states measured from the three non-encoded degrees of freedom, i.e. the wavelength, the polarization, and the arrival time. The probability distribution functions of arrival time and wavelength for optical pulses encoded different states can be calculated from measurements by the spectrum analyser and the optical detector. The polarization density matrixes for optical pulses encoded in different states can

be estimated from the measurements by the polarization analyser. The maximum absolute difference of the probability distribution functions or the maximum trace distance between the optical pulses encoded in different states over a specific non-encoded degree of freedom is calculated to give a verdict against the specified threshold.

If the quantum state is encoded in one of the above-mentioned three degrees of freedom, this degree of freedom shall be excluded from measurement under this EA. For example, if quantum states are encoded in polarization, then polarization density matrixes shall not be computed in this EA.

If the TX module under test is required to emit more than one intensity of optical pulse under the QKD protocol, the evaluator can use the time tags registered by the timing electronics to correlate the results of these measurement devices with the intensities emitted by the TX module. This allows the evaluator to generate a test result for each individual intensity level with the possible exception of any "vacuum" states where QKD protocols require a TX module to emit with a certain probability pulses of very small intensity.

7.6.2 Test procedure

The test procedure below is described for the case where the QKD protocol requires the TX module to emit optical pulses with a single intensity. If more than one intensity is required in the QKD protocol, the evaluator shall repeat the analysis in step 4 described below for each intensity setting (or each bin of intensity settings where the QKD protocol does not use a small set of discrete intensity settings), considering only the relevant encoded states in each analysis.

— Step 1: Turn on the TX module under test and configure it to emit pulses equivalent to those emitted in the raw data generation stage (apart from optionally their intensity if the internal attenuation is reduced during the measurement).

— Step 2: Measure the stream of optical pulses coming out of the TX module under test during an acquisition time with an optical detector, polarization analyser, and spectrum analyser. Use the timing electronics to time tag each of the outcomes with a progressive period number. The optical detector, the spectrum analyser, and the polarization analyser may alternatively be connected to the quantum channel output of the TX module at different times. If so, these measurements may utilize the same optical detector(s).

— Step 3: Where necessary, align the signal from the optical detector, polarization analyser, and spectrum analyser with the pattern of encoded states set by the TX module under test. For example, by using the digital data coming from the TX module under test and the time-tagged digital data coming from the timing electronics, the evaluator can cross-correlate the recorded outputs from the optical detector, polarization analyser, and spectrum analyser, respectively, with the pattern of encoded states coming from the TX module under test. This allows the evaluator to know what encoding setting was set by the TX module under test for the pulse present for each measurement by the optical detector, polarization analyser, and spectrum analyser.

— Step 4: Group all the results according to the state the TX module encoded.

  Calculate the maximum absolute difference in arrival time, t, between any two encoded states using Formula (12):

$$\delta_{\max,t} = \frac{1}{2}\max_{i\neq j}\left\{\sum_{t}|f(t,i)-f(t,j)|\right\} \tag{12}$$

  where

i and j are different encoded states;

f is the probability distribution function calculated from the group of results for the arrival time, t;

$\max\{\cdot\}$ is the maximum value in a set.

Calculate the maximum absolute difference in wavelength, λ, between any two encoded states using Formula (13):

$$\delta_{\max,\lambda} = \frac{1}{2}\max_{i\neq j}\left\{\sum_{\lambda}|g(\lambda,i)-g(\lambda,j)|\right\} \tag{13}$$

where

i and j are different encoded states;

g is the probability distribution function of the wavelength, λ;

$\max\{\cdot\}$ is the maximum value in a set.

Calculate the maximum absolute difference in the azimuthal angle, θ, of the major axis of polarization ellipse between any two encoded states using Formula (14):

$$\delta_{\max,\theta} = \frac{1}{2}\max_{i\neq j}\left\{\sum_{\theta}|p(\theta,i)-p(\theta,j)|\right\} \tag{14}$$

where

i and j are different encoded states;

p is the probability distribution function of the azimuthal angle, θ;

$\max\{\cdot\}$ is the maximum value in a set.

Calculate the maximum absolute difference in the ellipticity, ε, of the polarization ellipse (i.e. the ratio of the length of the semi-minor axis of the ellipse to the length of its semi-major axis) between any two encoded states using Formula (15):

$$\delta_{\max,\varepsilon} = \frac{1}{2}\max_{i\neq j}\left\{\sum_{\varepsilon}|q(\varepsilon,i)-q(\varepsilon,j)|\right\} \tag{15}$$

where

i and j are different encoded states;

q is the probability distribution function of the ellipticity, ε;

$\max\{\cdot\}$ is the maximum value in a set.

Fidelities between the different encoded states may be chosen in a PP or ST as an alternative measure of indistinguishability and the EA modified accordingly.

7.6.3 Pass/fail criteria

The test has passed if all of the following conditions are met. Otherwise, it has failed:

a) $\delta_{\max,t} < T_{\text{diffTime}}$;

b) $\delta_{\max,\theta} < T_{\text{diffAngle}}$;

c) $\delta_{\max,\varepsilon} < T_{\text{diffEllip}}$;

d) $\delta_{\max,\lambda} < T_{\text{diffSpec}}$.

If one of the above-mentioned three degrees of freedom is used in encoding quantum states by the TOE, the corresponding item of threshold comparison shall be excluded from the general pass/fail criteria.

NOTE This EA intends to evaluate the minimum requirements for checking the indistinguishability of encoded states in non-encoding degrees of freedom. It is possible that more non-encoding degrees of freedom are required to be tested for a specific TOE.

Table 9 lists the thresholds pertaining to the pass/fail decision of the EA.

Table 9 — Thresholds for the pass/fail decision of the EA

No.	Threshold notation	Meaning of the threshold
1	T_{diffTime}	The maximum absolute difference in time of arrival between the states encoded by the TX module.
2	T_{diffSpec}	The maximum absolute difference in spectrum between the states encoded by the TX module.
3	$T_{\text{diffAngle}}$	The maximum absolute difference in azimuthal angle of the polarization ellipse between the states encoded by the TX module.
4	$T_{\text{diffEllip}}$	The maximum absolute difference in the ellipticity between the states encoded by the TX module.

7.7 EA to test the uniform distribution of the global phase of optical pulses

7.7.1 General aspects

a) Objective of the evaluation activity

This EA intends to test if the optical pulses emitted by the TX module under test carry a random phase, which is a security requirement of a wide class of QKD protocols. The test outcome indicates whether the probability distribution of the measured relative phase between pulses is close, within the experimental uncertainty, to the expected theoretical distribution.

This EA as written is suitable for cases where the TX module under test can emit sufficient intensity for analogue intensities to be recorded meaningfully on the detectors. Where sufficient signal is not available from the TX module under test, the developer may propose modified or alternative EAs. For example, performing a set of statistical tests on a string of bits extracted from a similar measurement using single photon detectors.

For QKD protocols that do not require randomness of the global phase of each optical pulse, this EA is optional.

b) Required inputs

The developer shall provide the TX module under test, which is configured to emit pulses equivalent to those emitted in the raw data generation stage. The TX module under test shall allow the evaluator to access time tagged digital data containing the intensities and states encoded by the TX module during the test. The developer may optionally reduce attenuation inside the TX module under test to emit pulses at a higher average intensity level than in the raw data generation stage.

c) Required tool types and setup

The evaluator shall prepare an unbalanced Mach-Zehnder interferometer including one optical detector D. The arm length difference of the Mach-Zehnder interferometer should correspond to a time delay equal to the time between adjacent optical pulses (between adjacent reference pulses for the phase-

encoding system) emitted by the TX module under test. The arm length difference of the Mach-Zehnder interferometer should be stable to the order of tenths of the wavelength to keep a constant relative phase between the superposed pulses. The optical detectors should be chosen to have sufficient sensitivity to measure the output of the TX module under test. The Mach-Zehnder interferometer is connected to the quantum channel interface of the TX module under test. The transmittances of the two paths inside the Mach-Zehnder interferometer are assumed to be equal.

The evaluator shall also prepare timing electronics to time tag the output of the optical detector D and a tool for the digital time analysis of the digital data coming from the TX module under test and the timing electronics.

The schematic of the setup for this EA is shown in Figure 11.

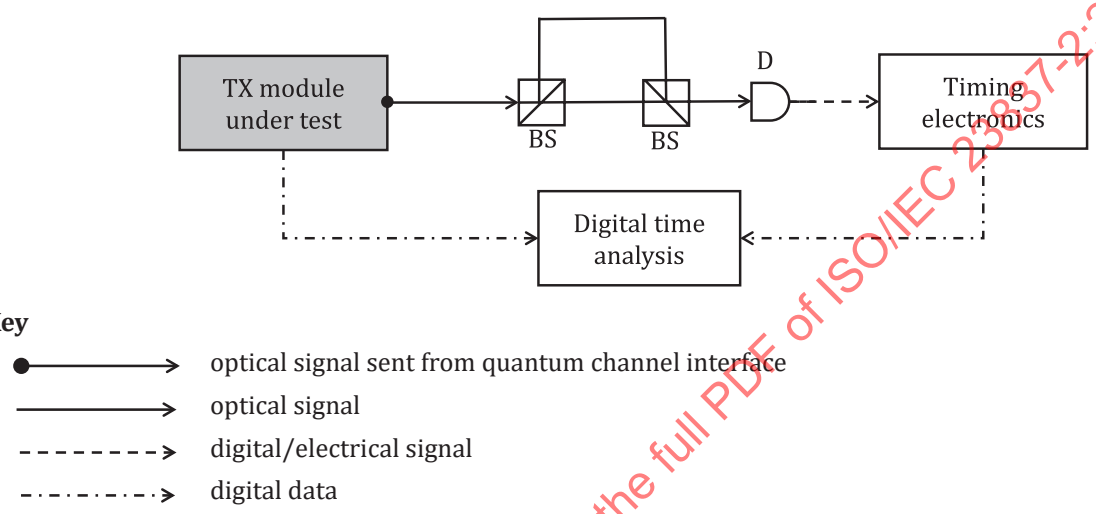


Figure 11 — Schematic of the setup for testing if the global phase of optical pulses is uniformly distributed

d) Rationale

This EA tests the randomness of the relative optical phase between consecutive optical pulses generated by the TX module under test. The probability distribution of intensity can be derived from the outputs of the Mach-Zehnder interferometer to indicate the phase distribution of the optical pulses emitted from the TX module under test. This probability distribution of intensity is compared with the theoretical uniform distribution to calculate the statistical distance, which can be used to give a verdict against a specified threshold.

7.7.2 Test procedure

The following description assumes that only one laser diode is used in the TX module under test. Where the TX module under test uses multiple laser diodes, the same test procedure shall be conducted for each laser diode separately.

— Step 1: Turn on the TX module under test and configure it to emit pulses equivalent to those in the raw data generation stage (apart from optionally their intensity if the internal attenuation is reduced during the measurement).

— Step 2: Measure the stream of the optical pulses coming out of the TX module under test after passing through the Mach-Zehnder interferometer with optical detector D. For some acquisition time, use the timing electronics to time tag each of the outcomes with a progressive period number.

— Step 3: Where necessary, align the digital strings from the optical detector with the pattern of encoded states set by the TX module under test. For example, by using the digital data coming from the TX module under test and the time-tagged digital data coming from the timing electronics, the evaluator can cross-correlate the pattern of encoded states and the intensity modulation coming

from the TX module under test with the results measured by the optical detector D. This allows the evaluator to know what state was encoded by the TX module under test for the pulse present for each measurement by the optical detector.

— Step 4: Select and group the measurement events where the interfering optical pulses arriving at the detector in the Mach-Zehnder interferometer were prepared in the same encoded state and intensity level. The data set is then filtered to keep only measurement results obtained from the most common combination of encoded intensity and state.

— Step 5: The final data set from step 4 is binned to produce a histogram described by the probabilities $p_{\mathrm{M}}(I)$ of the intensities recorded by the optical detector D arising from a given state and intensity level, where I represents the intensity bin-index.

— Step 6: Calculate the statistical distance between the measured probability distribution $p_{\mathrm{M}}(I)$ and the theoretically uniform distribution $p_{\mathrm{T}}(I)$ as shown in Formula (16):

$$d_{\mathrm{phase}} = \frac{1}{2}\sum_{I}\left|p_{\mathrm{M}}(I) - p_{\mathrm{T}}(I)\right|. \tag{16}$$

Evaluators may introduce detailed analysis to account for non-ideal characteristics of the measurement and detection system compared to the theoretical distribution expected in the real measurement system.

Although the statistical distance is applied in this EA to measure the deviation of the measured probability distribution from the theoretical distribution, some statistical tests for goodness of fit, such as the Kolmogorov-Smirnov test, may be used as alternative methods to test the randomness of the phase of the optical pulses.

7.7.3 Pass/fail criteria

If d_{phase} is smaller than the threshold $T_{\mathrm{maxDistPh}}$, the test has passed. Otherwise, it has failed.

Table 10 lists the threshold pertaining to the pass/fail decision of this EA.

Table 10 — Threshold for the pass/fail decision of the EA

No.	Threshold notation	Meaning of the threshold
1	$T_{\mathrm{maxDistPh}}$	The maximum tolerable deviation between the measured and the theoretical probability distributions pertaining to the intensities measured with an asymmetric Mach-Zehnder interferometer due to the relative phase of optical pulses when all optical pulses involved were encoded with the same state and intensity level.

7.8 EA to test the degree of optical isolation of the TX module

7.8.1 General aspects

a) Objective of the evaluation activity

This EA intends to test the isolation ability provided by the TX module under test against light injected from the quantum channel to the TX module. The amount of isolation is quantified for propagation in the opposite direction to that in which the quantum states are transmitted. It can therefore be an indicator as to whether the source of the TX module under test is protected against attacks such as Trojan-horse attacks, laser-seeding attacks, and laser damage attacks.

This EA as written is suitable for cases where a dedicated isolation component is implemented in the TOE.

b) Required inputs

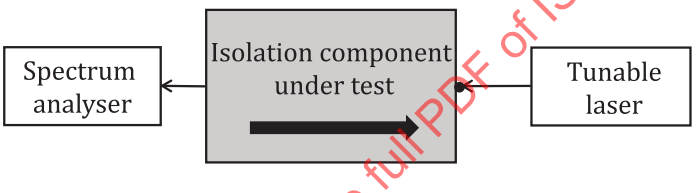
The developer shall provide the TX module under test enabling the direct testing of the internal isolation component or provide a dedicated isolation component of the same type as the one in the TX module under test.

c) Required tool types and setup

The evaluator shall prepare a tunable laser that can generate laser power, p, in the range of $[p_{min}, p_{max}]$. p_{max} shall be determined by consideration of the specific implementation of the TX module, e.g. by consideration of the threshold power at which an exceptional event of the TOE is indicated (see 7.9). Generally, p_{max} shall be lower than the power that would destroy the isolation component under test. The tunable laser can be operated in a wavelength range of $[\lambda_{min}, \lambda_{max}]$. The tunable laser is connected to the isolation component under test via the quantum channel interface of the TX module under test (or to the relevant interface of the dedicated isolation component when provided).

The evaluator shall prepare a spectrum analyser that works in the wavelength range of $[\lambda_{min}, \lambda_{max}]$. The spectrum analyser shall be chosen to have sufficient sensitivity to measure the output from the isolation component.

The schematic of the setup for this EA is shown in Figure 12.



Key

optical signal sent to quantum channel interface

optical signal

the forward direction of the isolation component

Figure 12 — Schematic of the setup for testing the degree of optical isolation of the TX module

d) Rationale

This EA tests the capability of isolating the injected light from the quantum channel into a TX module under test in a specified wavelength range. A laser is used to test the transmission of the isolation component. This laser can deliver powers up to a specified maximum power p_{max}, above which the TX module is protected by other means. For example, protection can be from an injected light monitor as in 7.9, or a component that fails safely above a specified power. The power measured by the spectrum analyser indicates the amount of power after the isolation component. The amount of isolation corresponding to a specific wavelength is calculated as the difference between the input and output power of the isolation component at the relevant wavelength. The minimum isolation is calculated over the specified wavelength range and can be used to give a verdict against a specified threshold.

Since it is generally inconvenient to measure the optical isolation by testing the entire TX module under test, this EA allows the input of an individual isolation component of the same type as the one in the TX module under test.

e) Dependencies

Where the TOE passes this EA, the necessity of conducting the EA specified in 7.10, which tests the robustness of the TOE against external laser injection, is determined by the evaluator.

7.8.2 Test procedure

— Step 1: Turn on the tunable laser at wavelength λ_{min}.

— Step 2: Set the power of the tunable laser to be p_{min}.

— Step 3: Denote the current power injected into the isolation component as p_{in}.

— Step 4: When the output power from the isolation component is stable, measure the output power by the spectrum analyser and record it at the current wavelength as p_{out}.

— Step 5: Calculate the isolation by $p_{iso} = p_{in} - p_{out}$, whose unit is dB.

— Step 6: Increase the laser power by a step of size, s_p, and repeat step 3 to step 5 until the laser power reaches p_{max}.

— Step 7: Increase the laser wavelength with by a step of size s_λ and repeat step 2 to step 6 until the wavelength reaches λ_{max}.

— Step 8: Compare the measured isolation p_{iso} for all different input powers and wavelengths and record the minimum isolation as p_{minIso}.

7.8.3 Pass/fail criteria

If the value of p_{minIso} is higher than the threshold T_{TXIso}, the test has passed. Otherwise, it has failed.

Table 11 lists the threshold pertaining to the pass/fail decision of the EA.

Table 11 — Threshold for the pass/fail decision of the EA

No.	Threshold notation	Meaning of the threshold
1	T_{TXIso}	The minimum isolation required for the isolation component under test in the TX module.

7.9 EA to test the sensitivity of the injected light monitor in the TX module

7.9.1 General aspects

a) Objective of the evaluation activity

This EA intends to test the effectiveness of the injected light monitor (or "monitor" in short hereinafter in this EA) in the TX module under test and whether the monitor indicates an exceptional event as a response to the light injection. The testing outcome indicates whether the monitor is sufficiently sensitive to detect attacks through injecting light into the TX module under test, e.g. Trojan-horse attack, laser seeding attack, and laser damage attack.

This EA only applies where the implementation of the TX module under test uses one or more optical detector(s) to place an upper bound on the power of light injected into the TX module from the quantum channel.

b) Required inputs

The developer shall provide the TX module under test, which is configured to emit pulses equivalent to those in the raw data generation stage. The TX module under test shall be able to indicate an exceptional event (e.g. an alarm) when the monitor detects injected light at a power that exceeds designed thresholds (i.e. $T_{TXMonPowerCW}$ and $T_{TXMonPowerPulse}$), as described in 7.9.3.

c) Required tool types and setup

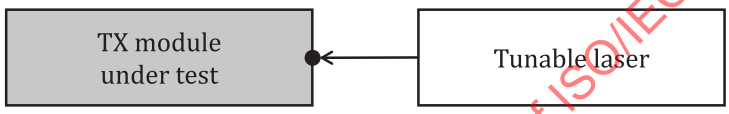
The evaluator shall prepare a tunable laser with a tunable wavelength in the range of $[\lambda_{min}, \lambda_{max}]$, this tunable laser should also satisfy the following conditions:

1) It should be able to generate continuous-wave emission with powers in the range of $[p_{minCW}, p_{maxCW}]$, where p_{maxCW} shall be less than the power that would destroy the monitor.

2) It should also be able to generate laser pulses with peak power in the range of $[p_{minPeak}, p_{maxPeak}]$, where $p_{maxPeak}$ shall be less than the power that would destroy the monitor. Their pulse width should be in the range of $[w_{min}, w_{max}]$, and output repetition frequency can be varied in the range of $[f_{min}, f_{max}]$.

Alternatively, it is possible to use two separate tunable lasers, where one operates in continuous-wave mode with the parameters mentioned in 1), and the other one operates in pulsed mode with the parameters mentioned in 2).

The testing tools are connected to the quantum channel interface of the TX module under test. The schematic of the setup for performing the EA is shown in Figure 13.



Key

optical signal sent to quantum channel interface

Figure 13 — Setup for testing the sensitivity of the injected light monitor in the TX module

d) Rationale

This EA verifies the effectiveness of the monitor in the TX module under test against laser injection. The tunable laser in the continuous-wave mode can be used to test the maximum power of injected continuous-wave emission without indicating an exceptional event. Likewise, the tunable laser in the pulsed mode can be used to test the maximum power of injected pulsed laser without indicating an exceptional event. By adjusting the characteristics of the tunable laser output, the response of the monitor to signals with different wavelengths, frequencies and pulse widths can be tested. Based on the observation of an exceptional event being indicated or not, the maximum power of the laser over all repetition frequencies, wavelengths, and pulse widths received by the monitor without it indicating an exceptional event can be calculated. Then, the calculated maximum power of the laser is used to give a verdict against a specified threshold.

This EA describes how to scan each input parameter with a certain step size to test the whole parameter space. However, considering the practical efficiency of conducting the test, these input parameters may be sampled with a random probing method.

e) Dependencies

This EA shall be considered and conducted together with the EAs specified in 7.8 and 7.10. If the TOE passes this EA, the EA of 7.10 shall still be conducted, since the dedicated monitor has a minimum sensitive power, below which the monitor does not work, so powers lower than the monitor's sensitivity shall still be tested in the EA of 7.10.

7.9.2 Test procedure

— Step 1: Turn on the TX module under test and configure it to emit pulses equivalent to those in the raw data generation stage.

— Step 2: Turn on the tunable laser at wavelength λ_{min} and set it to work in the continuous-wave mode.

— Step 3: Gradually increase the laser power from p_{minCW} to p_{maxCW}, until the monitor indicates an exceptional event, and record the value of power as p_{cw} for which the exception was indicated.

— Step 4: Increase the wavelength of the tunable laser by a step of size s_{λ} and repeat step 3 until the wavelength reaches λ_{max}. Calculate the maximum value of p_{cw} over all wavelengths and denote it by $p_{\text{maxCWcont}}$.

— Step 5: Switch the working mode of the laser to pulsed mode and set the repetition frequency of laser pulses to be f_{min} at wavelength λ_{min} with pulse width w_{min}.

— Step 6: Gradually increase the power of the pulsed laser from p_{minPeak} to p_{maxPeak}, and record the value of peak power p_{pulse} for which the monitor indicates an exceptional event.

— Step 7: Increase the repetition frequency of the laser by a step of size, s_{f}, and repeat step 6 until the repetition frequency reaches f_{max}.

— Step 8: Increase the wavelength of the laser by a step of size, s_{λ}, and repeat steps 6 and 7 until the wavelength reaches λ_{max}.

— Step 9: Increase the width of laser pulses by a step of size, s_{w}, and repeat steps 6 to 8 until the width of laser pulses reaches w_{max}.

— Step 10: Calculate the maximum value of p_{pulse} over all repetition frequencies, wavelengths, and pulse widths. Denote it by p_{maxPulse}.

7.9.3 Pass/fail criteria

If $p_{\text{maxCWcont}}$ is higher than the threshold $T_{\text{TXMonPowerCW}}$, or p_{maxPulse} is higher than the threshold $T_{\text{TXMonPowerPulse}}$, the test has failed. Otherwise, it has passed.

Table 12 lists the thresholds pertaining to the pass/fail decision of the EA.

Table 12 — Thresholds for the pass/fail decision of the EA

No.	Threshold notation	Meaning of the threshold
1	$T_{\text{TXMonPowerCW}}$	The threshold power at which the injected light monitor indicates an exceptional event when bright continuous-wave emission is injected into the TX module under test.
2	$T_{\text{TXMonPowerPulse}}$	The threshold peak power at which the injected light monitor indicates an exceptional event when bright pulse light emission is injected into the TX module under test.

7.10 EA to test the robustness of the TX module against laser injection

7.10.1 General aspects

a) Objective of evaluation activity

This EA intends to test the robustness of the TX module under test against laser light injected through the quantum channel interface. The testing outcome indicates whether the injected laser amends the characteristics of the TX module under test, which can create security flaws that potentially enable laser damage attacks or laser-seeding attacks.

b) Required inputs

The developer shall provide the TX module under test, which is configured to emit pulses equivalent to those emitted in the raw data generation stage. The TX module under test shall allow the evaluator to

access time tagged digital data containing the intensities and states encoded by the TX module during the test. The developer may optionally reduce the value of attenuation inside the TX module under test to emit pulses at a higher average intensity level than in the raw data generation stage.

c) Required tool types and setup

The evaluator shall prepare tunable laser with a tunable wavelength in the range of $[\lambda_{min}, \lambda_{max}]$, this tunable laser should also satisfy the following conditions:

1) It should be able to generate continuous-wave emission with powers in the range of $[p_{minCW}, p_{maxCW}]$.

2) It should also be able to generate laser pulses with peak power in the range of $[p_{minPeak}, p_{maxPeak}]$, and with a pulse width in the range of $[w_{min}, w_{max}]$, and whose output repetition frequency can be varied in the range of $[f_{min}, f_{max}]$.

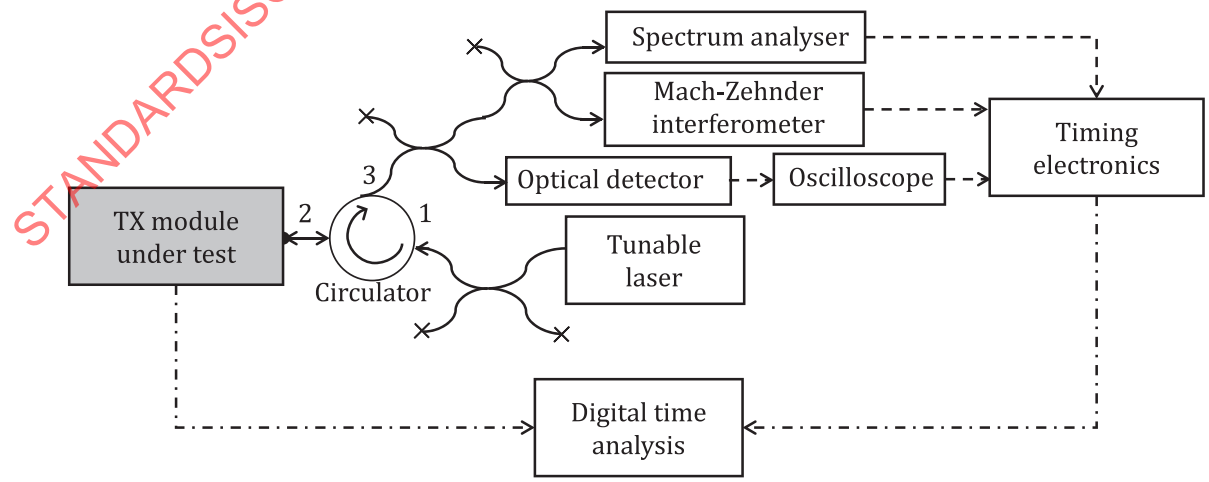
Alternatively, it is possible to use two separate tunable lasers, where one operates in continuous-wave mode with the parameters mentioned in 1), and the other one operates in pulsed mode with the parameters mentioned in 2).

If the TOE adopts a dedicated injected light monitor detecting the laser injection, p_{maxCW} and $p_{maxPeak}$ shall be higher than the thresholds $T_{TXMonPowerCW}$ and $T_{TXMonPowerPulse}$ defined in 7.9 respectively, but lower than powers that can destroy components and internal connections.

The evaluator shall also prepare measurement devices, such as a spectrum analyser, an oscilloscope, and a Mach-Zehnder interferometer. All the measurement devices should be chosen to have sufficient sensitivity to measure the output of the TX module under test. Furthermore, the difference in the arm lengths of the Mach-Zehnder interferometer should be stable to the order of tenths of the wavelength to keep a constant relative phase between the superposed pulses. Testing tools are connected to the quantum channel interface of the TX module under test.

The evaluator shall also prepare timing electronics to time tag the output of the oscilloscope, spectrum analyser, and Mach-Zehnder interferometer and a tool for the digital time analysis of the digital data coming from the TX module under test and the timing electronics. The optical detector, the spectrum analyser, and the Mach-Zehnder interferometer may alternatively be connected to the quantum channel output of the TX module under test at different times. If so, these measurements may utilize the same optical detector(s).

The schematic of the setup for this EA is shown in Figure 14.



Key

optical signal sent from quantum channel interface

optical signal sent to quantum channel interface

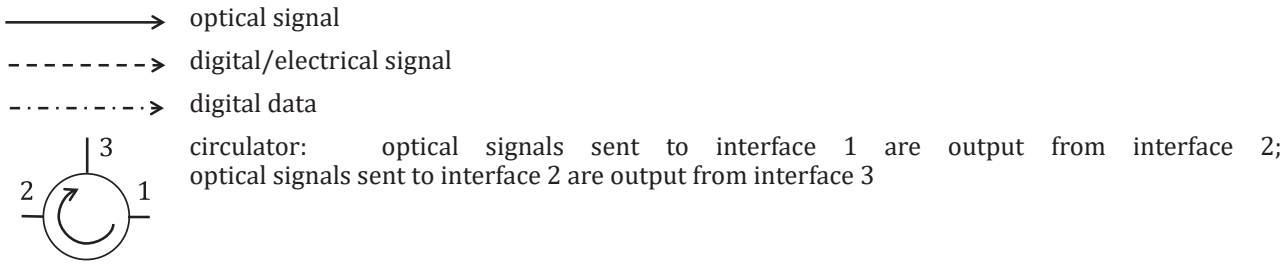


Figure 14 — Schematic of the setup for testing the robustness of the TX module against laser injection

d) Rationale

This EA aims to test the robustness of the TX module under test against laser injection by characterizing the differences over all emitted pulses in intensity, waveform, wavelength, and phase distribution with or without laser injection through the quantum channel. The tunable laser is able to work at the continuous-wave mode (or pulsed mode) to test the robustness of the TX module under test against continuous-wave emission injection (or pulsed laser injection respectively) with different wavelength, power, pulse width and frequency settings (pulse width and frequency settings apply only to the pulsed laser). The tunable laser can also be operated with a specified maximum power, which limits the highest amount of power an adversary can inject into the TX module under test without destroying components and their internal connections.

Based on the measurements by the oscilloscope and spectrum analyser, normalized intensity distributions of each encoded state before and after laser injection are measured in the time and frequency domains, respectively. Then, for each encoded state and each domain, the difference between the normalized intensity distributions before and after laser injection can be computed.

Based on the output of Mach-Zehnder interferometer, the intensity probability distribution of each of the encoded states before and after laser injection are measured, respectively. Then, for each encoded state, the difference between the phase distribution before and after laser injection can be computed.

The computation of the above difference in intensity distributions is iterated for different wavelength, power, frequency and pulse width combinations of the injected laser(s). The differences are characterized by statistical distances in this EA. The maximum difference of all cases is finally used to give a verdict against the specified thresholds.

If the TX module under test is required to emit optical pulses with more than one intensity under the QKD protocol, the evaluator can use the time tags registered by the timing electronics to correlate the results of these measurement devices with the intensities emitted by the TX module under test. This allows the evaluator to generate a test result for each individual intensity level with the possible exception of any "vacuum" states where QKD protocols require a TX module to emit with a certain probability pulses of very small intensity.

7.10.2 Test procedure

The following description assumes that only one laser diode is used in the TX module under test. For the TX module under test that uses multiple laser diodes, the same test procedure shall be conducted for each laser diode separately.

The test procedure is described for the case where the QKD protocol requires the TX module to emit optical pulses with a single intensity. If more than one intensity is emitted, the evaluator shall repeat the analysis in steps 4 to 18 described below for each intensity setting (or each bin of intensity settings

where the QKD protocol does not use a small set of discrete intensity settings), considering only the relevant encoded states in each analysis.

— Step 1: Turn on the TX module under test and configure it to emit pulses equivalent to those in the raw data generation stage. The attenuation of the optical pulses inside the TX module under test may be reduced by a measured amount, η, whose unit is dB, to aid the measurement of the signal pulses.

— Step 2: Measure the stream of the optical pulses coming out of the TX module under test during an acquisition time with the spectrum analyser, Mach-Zehnder interferometer, and oscilloscope. Use the timing electronics to time tag each of the outcomes with a progressive period number.

— Step 3: Where necessary, align the signal from the spectrum analyser, Mach-Zehnder interferometer, and the oscilloscope respectively with the pattern of encoded states set by the TX module under test. For example, by using the digital data coming from the TX module under test and the time-tagged digital data coming from the timing electronics, the evaluator can cross-correlate the recorded outputs from the spectrum analyser, Mach-Zehnder interferometer, and the oscilloscope with the pattern of encoded states coming from by the TX module under test. This allows the evaluator to know what state was encoded by the TX module under test for the pulse present for each measurement by these measurement devices.

— Step 4: Group all the measurement results from the oscilloscope and the spectrum analyser according to the state the TX module encoded. Record the intensities measured by the oscilloscope and calculate its normalized intensity distributions in the time domain $P_{\text{ref}}^{(i)}(t)$; record the spectrum measured by the spectrum analyser and calculate its normalized intensity distributions in the frequency domain $P_{\text{ref}}^{(i)}(\lambda)$, where the superscript i represents an encoded state; and t and λ represents the time and wavelength bin-index respectively.

— Step 5: For the measurement results from the Mach-Zehnder interferometer, select and group the measurement events where the interfering optical pulses arriving at the detectors in the Mach-Zehnder interferometer encoded with the same state.

— Step 6: The data sets from step 5 are binned to produce histograms described by the probabilities $P_{\text{ref}}^{(i)}(I)$ of the intensities recorded by one optical detector in the Mach-Zehnder interferometer, where the superscript i represents an encoded state; and I represents the intensity bin-index.

— Step 7: Turn on the tunable laser at wavelength $\lambda_{\min}$ and set it to work in the continuous-wave mode.

— Step 8: Set the power of the tunable laser to be $p_{\min \text{CW}}$.

— Step 9: Repeat step 4 to step 6, to record the intensities measured by the oscilloscope and calculate its normalized intensity distributions in time domain $P^{(i)}(t)$. Record the spectrum measured by the spectrum analyser and calculate its normalized intensity distributions in frequency domain $P^{(i)}(\lambda)$. Produce a histogram described by the probabilities $P^{(i)}(I)$ of the intensities recorded by one optical detector in the Mach-Zehnder interferometer.

— Step 10: Calculate the statistical distance between $P_{\text{ref}}^{(i)}(t)$ and $P^{(i)}(t)$ with Formula (17):

$$d_{\text{int}} = \frac{1}{2}\max_{i}\left\{\sum_{t}\left|P_{\text{ref}}^{(i)}(t) - P^{(i)}(t)\right|\right\} \tag{17}$$

where $\max\{\cdot\}$ is the maximum value in a set.

Calculate the statistical distance between $P_{\text{ref}}^{(i)}(\lambda)$ and $P^{(i)}(\lambda)$ by using Formula (18):

$$d_{\text{spec}} = \frac{1}{2}\max_i \left\{ \sum_{\lambda} \left| P_{\text{ref}}^{(i)}(\lambda) - P^{(i)}(\lambda) \right| \right\} \tag{18}$$

where $\max\{\cdot\}$ is the maximum value in a set.

Calculate the statistical distance between $P_{\text{ref}}^{(i)}(I)$ and $P^{(i)}(I)$ by Formula (19):

$$d_{\text{phase}} = \frac{1}{2}\max_i \left\{ \sum_{I} \left| P_{\text{ref}}^{(i)}(I) - P^{(i)}(I) \right| \right\} \tag{19}$$

where $\max\{\cdot\}$ is the maximum value in a set.

Although the statistical distance is applied in this EA to measure the deviation of two measured probability distributions, some nonparametric statistical tests, such as the Kolmogorov-Smirnov test, may be used as alternative methods to realize the same objective.

— Step 11: Increase the injection laser power by a step of size, s_{p}, and repeat from steps 9 to 10 until the power reaches $p_{\text{maxCW}} - \eta$, where the powers are expressed in dB.

— Step 12: Increase the wavelength by a step of size, s_{λ}, and repeat steps 9 to 11 until the wavelength reaches λ_{max}.

— Step 13: Switch the working mode of the tunable laser to pulsed mode, set the peak power of laser pulses to be p_{minPeak}, and its repetition frequency to be f_{min} at wavelength λ_{min} with pulse width w_{min}.

— Step 14: Increase the peak power by a step of size s_{peak} and repeat steps 9 and 10 until the peak power reaches $p_{\text{maxPeak}} - \eta$, where the powers are expressed in dB.

— Step 15: Increase the repetition frequency of the laser by a step of size, s_{f}, and repeat step 14 until the repetition frequency reaches f_{max}.

— Step 16: Increase the wavelength of the laser by a step of size, s_{λ}, and repeat steps 14 to 15 until the wavelength reaches λ_{max}.

— Step 17: Increase the width of laser pulses by a step of size, s_{w}, and repeat steps 14 to 16 until the width of laser pulses reaches w_{max}.

— Step 18: Calculate the maximum d_{int} and denote it by d_{maxInt}. Calculate the maximum d_{spec} and denote it by d_{maxSpec}. Calculate the maximum d_{phase} and denote it by d_{maxPhase}. These maximums are calculated over all the tests both in continuous wave mode and pulsed mode.

7.10.3 Pass/fail criteria

The test has passed if all of the following conditions are met. Otherwise, it has failed:

a) $d_{\text{maxInt}} < T_{\text{powerInj}}$;

b) $d_{\text{maxSpec}} < T_{\text{specShift}}$;

c) $d_{\text{maxPhase}} < T_{\text{phChange}}$.

Table 13 lists the thresholds pertaining to the pass/fail decision of the EA.

Table 13 — Thresholds for the pass/fail decision of the EA

No.	Threshold notation	Meaning of the threshold
1	T_{powerInj}	Maximum tolerable pulse intensity deviation caused by laser injection
2	$T_{\text{specShift}}$	Maximum tolerable pulse spectrum deviation caused by laser injection
3	T_{phChange}	Maximum tolerable pulse phase deviation caused by laser injection

8 EAs for the evaluation of quantum optical components in the receiver module

8.1 General

The EAs for the evaluation of quantum optical components in the RX module are listed in Table 14. These EAs address potential flaws in quantum optical components of QKD modules that, if present, can otherwise compromise the security functions realizing the two security requirements FPT_EMS.1/Quantum and FPT_PHP.3. These flaws are known security-related issues of (or attacks against) RX modules that have been published and peer reviewed in the academic literature. Although not all of them have been demonstrated to date, a strategy for each type of attack has been reported.

Table 14 — EAs for the evaluation of quantum optical components in an RX module

Evaluation activity	Description	SFRs correspondence	Subclause index	Applicable protocols
Test the consistency of detection probability in the RX module	Test if the detection probabilities output from the RX module under test are consistent with the model of the implemented QKD protocol.	FPT_EMS.1/Quantum	8.2	DV-PM-QKD; DV-EB-QKD
Test information leakage of back-flashes from the RX module	Test if the RX module under test emits photons back into the quantum channel, which yields information about the detected state after the detection of a photon	FPT_EMS.1/Quantum	8.3	DV-PM-QKD; DV-EB-QKD
Test the degree of optical isolation of the RX module	Test if the isolation ability provided by the RX module under test suffices to prevent light reflecting back from the tested module to the quantum channel.	FPT_PHP.3	8.4	DV-PM-QKD; DV-EB-QKD; CV-PM-QKD; CV-EB-QKD
Test the sensitivity of the injected light monitor in the RX module	Test if the injected light monitor deployed to detect light injected through the quantum channel interface works properly.	FPT_PHP.3	8.5	DV-PM-QKD; DV-EB-QKD; CV-PM-QKD; CV-EB-QKD
Test the robustness of the RX module against bright light blinding	Test if the detection output of the RX module under test is able to be controlled by injected bright light.	FPT_PHP.3	8.6	DV-PM-QKD; DV-EB-QKD
Test the appropriateness of dead time settings of single-photon detectors	Test if the raw data generated by the RX module under test excludes any detection events generated during the dead time period of any of the SPDs.	FPT_PHP.3	8.7	DV-PM-QKD; DV-EB-QKD
NOTE Depending on the implemented QKD protocols, not all the EAs are necessary for a specific TOE.				

Table 14 *(continued)*

Evaluation activity	Description	SFRs correspondence	Subclause index	Applicable protocols
Test the temporal profile of the detection efficiency for single-photon detectors	Test if the temporal profile of the detection efficiency when detecting pulses at the single-photon level is the same as that of detecting pulses at higher average photon numbers for each SPD.	FPT_PHP.3	8.8	DV-PM-QKD; DV-EB-QKD
Test the robustness of the RX module against laser injection	Test if the detection probability of the RX module under test can be altered by shining additional light into the RX module under test through the quantum channel interface.	FPT_PHP.3	8.9	DV-PM-QKD; DV-EB-QKD;
Test the detection limits of homodyne detectors in the RX module	Test if an RX module under test rejects the data or reports an exceptional event once the homodyne detector operates in the saturation region.	FPT_PHP.3	8.10	CV-PM-QKD; CV-EB-QKD
Test the appropriateness of double-click event handling	Test if double click events are properly handled during the post-processing stage, e.g. by randomly assigning a bit value to these events.	FPT_PHP.3	8.11	DV-PM-QKD; DV-EB-QKD
NOTE Depending on the implemented QKD protocols, not all the EAs are necessary for a specific TOE.				

a) General description of inputs

The RX module should be operated under conditions that are as close to normal operating conditions as possible, which means the security test procedures should be conducted on the RX module as a whole, without requiring additional interfaces, channels, or outputs other than those already present on the RX module. Its objective is to reflect the security status of actual QKD modules under the conditions they can face in operation.

When planning the tests and analysing the results, the details of the performance of the detector(s) in the RX module under test should be considered, including dark counts, after pulses, time jitter, more than one detection event occurring for one input state, all of which can occur during measurements. Any corrections made to account for the non-ideal behaviour of instruments shall be reasonable and care shall be taken to ensure that corrections are performed in a manner that does not compromise the objectives of the EAs.

Generally, the EAs in Clause 8 require that the RX module under test works in the raw data generation stage, such that the RX module under test can detect and measure the test states.

In order to conduct the EM effectively, EAs may allow more modifications to the TOE, for example:

— In a limited number of instances, if the information gained from measuring the whole system is insufficient, individual components or sub-assemblies of the RX module under test may be tested (see 8.4).

— Time tagged digital data output from the RX module under test may be enabled where needed to analyse the encoded states corresponding to the raw data (see 8.3 and 8.7).

— The detection count rates output from the RX module under test may be required to be accessible. Alternatively, the RX module under test may provide time tagged data about detection events since detection count rates can be derived from such data.

— A special configuration of an RX module under test may be used, e.g. to ignore repeated failures without transitioning to a failure state for the duration of an EA.

Where an EA requires a modification to the operation of an RX module under test, the modification should be specified in the description of required inputs of the EA. It is implicitly assumed that the modification is removed or disabled after testing.

b) General description of test tools and setup

For EAs that require the RX module under test to work in the raw data generation stage, the test setup shall ensure the RX module under test can work in this stage. Some synchronization links between the RX module and test tools are typically needed to coordinate the whole setup.

Alternatively, it may be appropriate to introduce a TX emulator to provide the signals expected by the RX module to enable it to be operated as required. Specifically:

— Such a TX emulator may not be used to emit test states that can be generated by tools described in the EA.

— Test states may be required to be emitted at times that are fixed in relation to the times such states would be provided by a TX module in operation. In such cases, one option is for the TX emulator to supply trigger signals to other tools or to receive trigger signals from other tools.

— It may be practical to derive any timing signals required by test tools used in the EA from signals present in the optical link between the TX emulator and the RX module under test or for test tools to supply any necessary timing signals themselves independently.

— The optimal way to combine or split communications between a TX emulator and an RX module under test and signals to/from other tools depends upon the EA and details of the RX module under test. Optical couplers or wavelength multiplexing devices are usually suitable.

In some cases, a TX module under test may be used as a TX emulator.

8.2 EA to test the consistency of detection probability in the RX module

8.2.1 General aspects

a) Objective of the evaluation activity

This EA intends to test if the detection probabilities output from the RX module under test are consistent with the model of the implemented QKD protocol. In particular, the EA tests the response of the RX module under test when the arrival time and the wavelength of optical pulses received from the quantum channel are varied. The outcome of the test gives indications about the vulnerability of the RX module under test to attacks such as the time-shift attack, the detection-probability-mismatch attack, and the wavelength-dependent attack.

This EA is applicable when a mismatch in the detection probabilities of a pair of detectors in the RX module under test threatens security.

b) Required inputs

The developer shall provide the RX module under test working in the raw data generation stage. The RX module under test shall allow access to the count rates of detection events corresponding to each input state measured by the RX module. This means providing access to one count rate for each state at the input from the quantum channel for which the RX module performs measurement(s). One such count

rate includes all relevant detection events that are considered by the RX module to be measurements of a particular input state under the QKD protocol.

NOTE 1 Some RX modules change the configuration of the decoding optics over time to alter the detector(s) that a particular input state is intended to be delivered to. Multiple detectors can contribute relevant detection events to the count rate for a particular input state over time. At certain times an RX module can be configured not to contribute relevant detection events in any detector for a particular input state.

The developer shall also provide the intrinsic mismatches expected in the count rates for all pairs of measurements on input states that are performed by the RX module under test while receiving input states modulated randomly as prescribed by the encoding procedure of the analysed QKD protocol but at a constant mean photon number. For example, a QKD protocol may not involve the transmission of or measurement of states with equal probabilities.

c) Required tool types and setup

The evaluator shall prepare a tunable laser source that can generate laser pulses in a wavelength range of $[\lambda_{\min}, \lambda_{\max}]$ with an adjustable delay in the range of $[d_{\min}, d_{\max}]$ that covers the whole gate period of the detector, or the whole period between states output by the TX module under the QKD protocol for a detector that is not gated. An additional time-delay controller may be used to ensure the accuracy of delay adjustment.

A state modulator modulates the laser pulses into encoded states and outputs the basis choice information.

A variable attenuator attenuates laser pulses to a constant mean photon number, which is equal to that of a representative quantum state received by the RX module in the raw data generation stage. The variable attenuator is connected to the quantum channel interface of the RX module under test.

The quality of the test depends on the pulse width and the spectral width of the tunable laser. In a PP or an ST, the maximum pulse width and the maximum spectral width should be provided.

The schematic of the setup for performing the EA is shown in Figure 15.

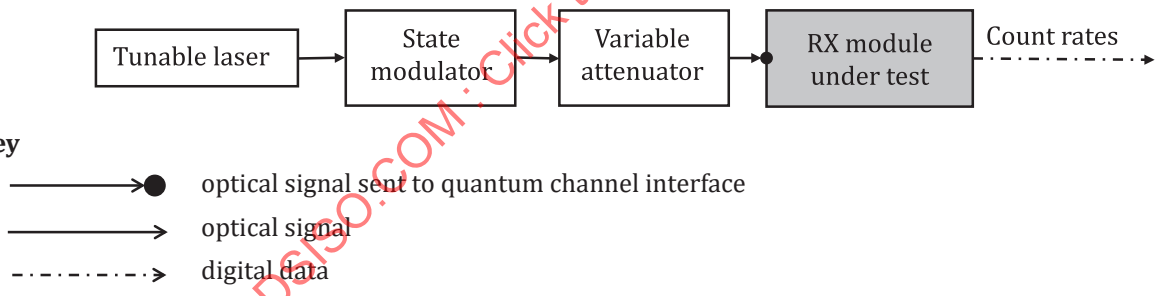


Figure 15 — Schematic of the setup for testing the consistency of detection probability

d) Rationale

This EA tests the response of the RX module under test to variations in the arrival time and wavelength of the optical pulses entering the RX module under test from the quantum channel. By adjusting the time delay and the wavelength of the optical pulses output from the tunable laser, the detection probability profiles in time and wavelength can be characterized. The obtained profiles can be used to calculate the detection probability mismatches of the RX module under test. The quantified detection probability mismatches are used to compare with the specified thresholds to give a verdict.

NOTE 2 This EA intends to evaluate the minimum requirements for testing the detection probability mismatch in the TOE. Depending on the practice, more degrees of freedom, e.g. the polarization, can be tested in a similar way for a specific TOE.

8.2.2 Test procedure

— Step 1: Turn on the RX module under test to work in the raw data generation stage.

— Step 2: Turn on the tunable laser and set it to emit pulses at wavelengths $\lambda_{\min}$ and time delay $d_{\min}$.

— Step 3: Adjust the state modulator to randomly modulate the optical pulses as prescribed by the encoding procedure of the analysed QKD protocol. Adjust the variable attenuator to attenuate the optical pulses to a constant mean photon number, which is equal to that of a representative quantum state received by the RX module in the raw data generation stage.

Random modulation in this step is optional. Alternatively, the encoded states may be modulated in a representative pattern.

— Step 4: Sequentially vary the wavelength of optical pulses emitted by the tunable laser in the range of $[\lambda_{\min}, \lambda_{\max}]$ with a step size, s_λ, and the time delay of optical pulses emitted by the tunable laser in the range of $[d_{\min}, d_{\max}]$ with a step size, s_d.

— Step 5: For each s_λ and s_d, record for an acquisition time to obtain the count rates output from the RX module under test, denoted by $C(s_\lambda, s_d, i)$ and $C(s_\lambda, s_d, j)$, where i, j refers to the i-th and j-th outputs respectively from the RX module under test, and $i \neq j$. This acquisition time shall be long enough that statistical errors in the measurement results are not likely to induce false detection probability mismatches that exceed the threshold.

— Step 6: Calculate the detection probability mismatch between any two encoded states using Formula (20):

$$\sigma^{(i,j)}(s_\lambda, s_d) = \left| \frac{C(s_\lambda, s_d, i) - C(s_\lambda, s_d, j)}{C(s_\lambda, s_d, i) + C(s_\lambda, s_d, j)} - \Delta_{i,j} \right| \tag{20}$$

where $\Delta_{i,j}$ is the intrinsic mismatch of the detection count rates between the i-th and the j-th outputs from the RX module under test, calculated in a similar manner as the difference of the expected rates divided by the sum for input pulses modulated as expected under the QKD protocol.

NOTE Such intrinsic mismatches typically occur when the QKD protocol implemented involves transmitting and/or performing measurements on each of the encoded states with unequal probabilities.

— Step 7: Calculate the maximum of $\sigma^{(i,j)}(s_\lambda, s_d)$ over all s_λ, s_d and outputs from the RX module under test, which is denoted by $\sigma_{\max}$.

8.2.3 Pass/fail criteria

If $\sigma_{\max}$ is smaller than the threshold $T_{\text{misDetProb}}$, the test has passed. Otherwise, it has failed.

Table 15 lists the threshold pertaining to the pass/fail decision of the EA.

Table 15 — Threshold for the pass/fail decision of the EA

No.	Threshold notation	Meaning of the threshold
1	$T_{\text{misDetProb}}$	The maximum tolerable mismatch between the detection probability responses in wavelength and time for the RX module under test that are required to be matched under the QKD protocol.

8.3 EA to test information leakage of back-flashes from the RX module

8.3.1 General aspects

a) Objective of the evaluation activity

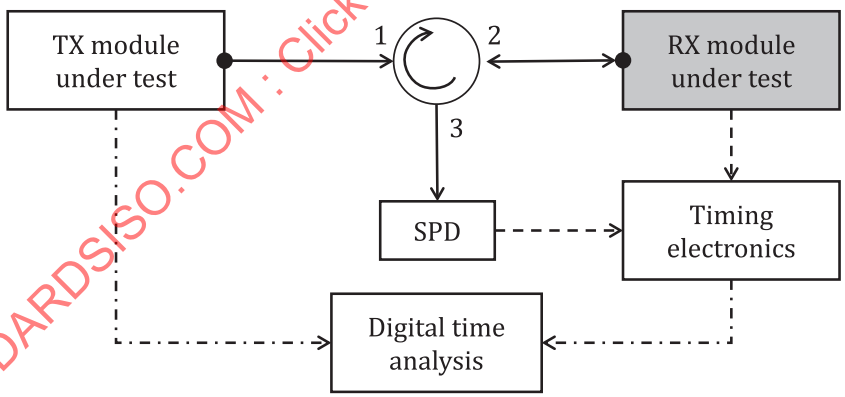
This EA intends to test if the RX module under test emits photons back into the quantum channel when it registers a detection. These photons are called "back-flashes" and potentially leak information from the RX module under test to the adversary if they carry information about the measurement outcome obtained by the RX module under test. This can arise if the back-flashes from different detectors in the RX module under test are distinguishable in any degree of freedom at an external port of the RX module under test. The testing outcome indicates whether the RX module under test can potentially leak significant information via back-flashes without considering whether any back-flashes present are distinguishable.

b) Required inputs

The developer shall provide an entire TOE, including the TX module under test and the RX module under test, working in the raw data generation stage. The TX module under test shall allow the evaluator to access time tagged digital data containing the intensities and states encoded by the TX module during the test. The RX module under test shall allow the evaluator to access time tagged raw data.

c) Required tool types and setup

The evaluator shall prepare a circulator, an SPD with known minimum detection efficiency η_{det} over a wavelength sensitive range of $[\lambda_{\mathrm{min}}, \lambda_{\mathrm{max}}]$ (which should be consistent with the values assigned in a PP or an ST), timing electronics to time tag the counts from the SPD and RX module under test, a tool for the digital time analysis to cross-correlate the output of the RX module under test and the SPD with the pattern of encoded states and intensity modulation emitted by the TX module under test, and other necessary fibre optic components. The circulator is connected to the quantum channel interface of the RX module under test. The transmittance η_{c23} from the RX module under test to the SPD shall be calibrated by the evaluator. The schematic of the setup for performing the EA is shown in Figure 16.



Key

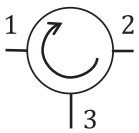
optical signal sent from quantum channel interface

optical signal sent to quantum channel interface

optical signal

digital/electrical signal

digital data



circulator: optical signals sent to interface 1 are output from interface 2; optical signals sent to interface 2 are output from interface 3

Figure 16 — Schematic of the setup for testing the back-flashes from the RX module

d) Rationale

This EA intends to verify if the RX module under test emits back-flashes into the quantum channel when it registers a detection. For that purpose, a circulator is used to direct back-flashes emitted by the RX module under test to an external SPD. The SPD and timing electronics on the one hand and the RX module under test on the other hand both record counts into two distinct digital data sets. Then, it is necessary to correlate the counts in these two digital data sets to calculate the back-flash probability for each encoded state and intensity level. The maximum back-flash probability over all encoded states and intensity levels is recorded to give a verdict against the specified threshold.

8.3.2 Test procedure

— Step 1: Turn on the TX module under test and the RX module under test. Let them work in the raw data generation stage.

— Step 2: Measure signals coming from the RX module under test in response to a stream of optical pulses coming out of the TX module under test during an acquisition time with an SPD of known efficiency, η_{det}. Use the timing electronics to time tag each of the outcomes with a progressive period number.

— Step 3: Align the digital strings coming from the SPD and from the RX module under test, so that the detection events in the two strings correspond to the same optical pulse emitted by the TX module under test. For example, by using the digital data coming from the TX module under test and the time-tagged digital data coming from the timing electronics, the evaluator can cross-correlate the quantum state and intensity modulation pattern coming from the TX module under test with the counts measured by the SPD and those measured by the RX module under test.

— Step 4: Referring to the given number of emitted optical pulses, count how many counts N_{BF} have been recorded by the SPD and how many counts N_{QKD} have been recorded by the RX module under test for each encoded state and intensity level.

— Step 5: Turn off the RX module under test, set the TX module under test as the status in steps 2 and 3, record the counts of SPD N_{BG} in the same acquisition time as in step 2. Recorded N_{BG} is caused by the light reflections from the test environment and dark counts of the SPD for each encoded state.

— Step 6: For each encoded state and intensity level, calculate the back-flash probability using Formula (21):

$$P_{\mathrm{BF}} = \frac{N_{\mathrm{BF}} - N_{\mathrm{BG}}}{N_{\mathrm{QKD}}\eta_{\mathrm{det}}\eta_{\mathrm{c23}}} \tag{21}$$

where

N_{BF} is the count number recorded by the SPD;

N_{BG} is the count number recorded by the SPD after turning off the RX module under test;

N_{QKD} is the count number recorded by the RX module under test;

η_{det} is the minimum detection efficiency of the SPD;

η_{c23} is the transmittance from the RX module under test to the SPD.

Record the value of back-flash probability maximized over all encoded states and intensity levels as $P_{\text{maxBF}} = \max\{P_{\text{BF}}\}$, where $\max\{\cdot\}$ is the maximum value in a set.

8.3.3 Pass/fail criteria

If P_{maxBF} is below a certain threshold value T_{PBF}, the test has passed. Otherwise, it has failed.

Table 16 lists the threshold pertaining to the pass/fail decision of the EA.

Table 16 — Threshold for the pass/fail decision of the EA

No.	Threshold notation	Meaning of the threshold
1	T_{PBF}	The maximum probability that a back-flash photon exits from the RX module under test when the RX module under test registers the detection of a photon.

8.4 EA to test the degree of optical isolation of the RX module

8.4.1 General aspects

a) Objective of the evaluation activity

This EA intends to test the total amount of isolation provided by the RX module under test if light reflects back from the tested module to the quantum channel. The amount of isolation is quantified for the direction that is backwards to the direction in which the quantum state is transmitted. This indicates whether the RX module under test prevents from attacks such as the Trojan-horse attack and the backflash attack.

This EA is suitable for cases where a dedicated isolation component is implemented in the TOE.

b) Required inputs

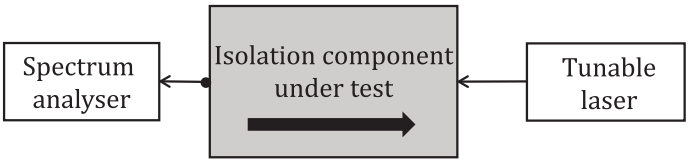
The developer shall provide the RX module under test, to enable direct testing of the internal isolation component. Alternatively, the developer shall provide a dedicated isolation component of the same type as the one in the RX module under test.

c) Required tool types and setup

The evaluator shall prepare a tunable laser that can generate laser power in the range of $[p_{\text{min}}, p_{\text{max}}]$. p_{max} shall be determined by consideration of the specific implementation of the RX module, e.g. by consideration of the threshold power at which an exceptional event of the TOE is indicated (see 8.5). Generally, p_{max} shall be lower than the power that would destroy the isolation component under test. The tunable laser can be operated in a wavelength range of $[\lambda_{\text{min}}, \lambda_{\text{max}}]$.

The evaluator shall prepare a spectrum analyser that works in the wavelength range of $[\lambda_{\text{min}}, \lambda_{\text{max}}]$. The spectrum analyser shall be chosen to have sufficient sensitivity to measure the output of the isolation component. The spectrum analyser is connected to the isolation component under test via the quantum channel interface of the isolation component under test.

The schematic of the setup for this EA is shown in Figure 17.



Key

optical signal sent from quantum channel interface

optical signal

the forward direction of the isolation component

Figure 17 — Schematic of the setup for testing the degree of optical isolation of the RX module

d) Rationale

This EA shows the capability of isolating the reflected light from an RX module under test back to the quantum channel in a specified wavelength range. A laser is used to test the transmission of the isolation component. This laser is able to deliver powers up to a specified maximum power, p_{max}, above which the RX module is protected by other means. For example, protection can be from an injected light monitor as in 7.9, or a component that fails safely above a specified power. The power measured by the spectrum analyser indicates the amount of power after the isolation component. The amount of isolation corresponding to a specific wavelength is calculated by the difference between the input and output power of the isolation component at such wavelength. The minimum isolation is calculated over the specified wavelength range and it can be used to give a verdict against a specified threshold.

Since it is generally inconvenient to measure the optical isolation by testing the entire RX module under test, this EA requires the input of an individual isolation component that is of the same type as the one in the RX module under test.

8.4.2 Test procedure

— Step 1: Turn on the tunable laser at wavelength λ_{min}.

— Step 2: Set the power of the tunable laser to be p_{min}.

— Step 3: Denote the current power injected into the isolation component as p_{in}.

— Step 4: When the output power from the isolation component is stable, measure the output power by the spectrum analyser and record it at the current wavelength as p_{out}.

— Step 5: Calculate the isolation by $p_{iso} = p_{in} - p_{out}$, whose unit is dB.

— Step 6: Increase the laser power by a step of size, s_p, and repeat step 3 to step 5 until the laser power reaches p_{max}.

— Step 7: Increase the laser wavelength by a step of size, s_λ, and repeat step 2 to step 6 until the wavelength reaches λ_{max}.

— Step 8: Compare the measured isolation p_{iso} for all combinations of input power and wavelength and record the minimum isolation as p_{minIso}.

8.4.3 Pass/fail criteria

If the value of p_{minIso} is higher than the threshold T_{RXIso}, the test has passed. Otherwise, it has failed.

Table 17 lists the threshold pertaining to the pass/fail decision of the EA.

Table 17 — Threshold for the pass/fail decision of the EA

No.	Threshold notation	Meaning of the threshold
1	T_{RXIso}	The minimum isolation required for the isolation component under test in the RX module.

8.5 EA to test the sensitivity of the injected light monitor in the RX module

8.5.1 General aspects

a) Objective of the evaluation activity

This EA intends to test the effectiveness of the injected light monitor (or "monitor" in short hereinafter in this EA) in the RX module under test and whether the monitor indicates an exceptional event as a response to the light injection. The testing outcome indicates whether the monitor is sufficiently sensitive to detect attacks, e.g. Trojan-horse attack and detector-control attacks, which involve the injection of light into the RX module under test before other protective measures are compromised, etc.

This EA only applies where the implementation of the RX module under test uses one or more monitor(s) to place an upper bound on the power of light injected into the RX module from the quantum channel.

b) Required inputs

The developer shall provide an RX module under test working in raw data generation stage. The RX module under test shall be able to indicate an exceptional event (i.e. an alarm) when the monitor detects an injected laser whose power exceeds designed thresholds (i.e. $T_{\mathrm{RXMonPowerCW}}$ and $T_{\mathrm{RXMonPowerPulse}}$), as described in 8.5.3.

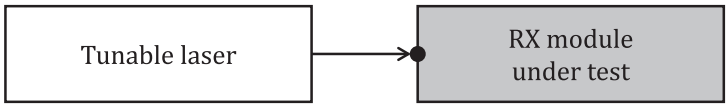
c) Required tool types and setup

The evaluator shall prepare a tunable laser with a tunable wavelength in the range of $[\lambda_{\min}, \lambda_{\max}]$, this tunable laser should also satisfy the following conditions:

1) It should be able to generate a continuous-wave emission with powers in the range of $[p_{\mathrm{minCW}}, p_{\mathrm{maxCW}}]$, where p_{maxCW} shall be less than the power that would destroy the monitor.
2) It should also be able to generate laser pulses with peak power in the range of $[p_{\mathrm{minPeak}}, p_{\mathrm{maxPeak}}]$, where p_{maxPeak} shall be less than the power that would destroy the monitor. Their pulse width should be in the range of $[w_{\min}, w_{\max}]$, and output repetition frequency can be varied in the range of $[f_{\min}, f_{\max}]$.

Alternatively, it is possible to use two separate tunable lasers, where one operates in continuous-wave mode with the parameters mentioned in 1), and the other one operates in pulsed mode with the parameters mentioned in 2).

The testing tools are connected to the quantum channel interface of the RX module under test. The schematic of the setup for performing the EA is shown in Figure 18.



Key

optical signal sent to quantum channel interface

Figure 18 — Setup for testing the sensitivity of the injected light monitor in the RX module

d) Rationale

This EA verifies the effectiveness of the monitor in the RX module under test against laser injection. The tunable laser operating in the continuous-wave mode can be used to test the maximum power of injected continuous-wave emission without indicating an exceptional event. Likewise, the tunable laser operating in the pulsed mode can be used to test the maximum power of injected pulsed laser without indicating an exceptional event. By adjusting the characteristics of the tunable laser output, the response of the monitor to signals with different wavelengths, frequencies and pulse widths can be tested. Based on the observation of exceptional event being indicated or not, the maximum power of the laser over all repetition frequencies, wavelengths, and pulse widths received by the monitor without it indicating an exceptional event can be calculated. Then, the calculated maximum power of the laser is used to give a verdict against a specified threshold.

This EA describes how to scan each input parameter with a certain step size to test the whole parameter space. However, considering the practical efficiency of conducting the test, these input parameters may be sampled with a random probing method.

e) Dependencies

This EA shall be considered and conducted together with the EAs in 8.6 and 8.9. If the TOE passes this EA, the EAs in 8.6 and 8.9 shall still be conducted, since there is some minimum power below which a dedicated monitor is not sensitive. Powers lower than the monitor's sensitivity shall still be tested in the EAs in 8.6 and 8.9.

8.5.2 Test procedure

— Step 1: Turn on the RX module under test and let it work in the raw data generation stage.

— Step 2: Turn on the tunable laser at wavelength λ_{min} and set it to work in continuous-wave mode at power, p_{minCW}.

— Step 3: Gradually increase the laser power from p_{minCW} to p_{maxCW}, and record the power p_{cw} when the monitor indicates an exceptional event.

— Step 4: Increase the wavelength of the tunable laser by a step of size s_{λ} and repeat step 3 until the wavelength reaches λ_{max}. Calculate the maximum value of p_{cw} over all wavelengths and denote it by $p_{\text{maxCWcont}}$.

— Step 5: Switch the working mode of the laser to pulsed mode and set the repetition frequency of laser pulses to be f_{min} at wavelength λ_{min} with pulse width w_{min}.

— Step 6: Gradually increase the power of the pulsed laser from p_{minPeak} to p_{maxPeak}, and record the value of peak power p_{pulse} when the monitor indicates an exceptional event.

— Step 7: Increase the repetition frequency of laser by a step of size s_{f} and repeat step 6 until the repetition frequency reaches f_{max}.

— Step 8: Increase the wavelength of the laser by a step of size s_{λ} and repeat steps 6 and 7 until the wavelength reaches λ_{max}.

— Step 9: Increase the width of laser pulses by a step of size s_{w} and repeat steps 6 to 8 until the width of laser pulses reaches w_{max}.

— Step 10: Calculate the maximum value of p_{pulse} over all repetition frequencies, wavelengths, and pulse widths, and denote it by p_{maxPulse}.

8.5.3 Pass/fail criteria

If $p_{\text{maxCWcont}}$ is higher than the threshold $T_{\text{RXMonPowerCW}}$, or p_{maxPulse} is higher than the threshold $T_{\text{RXMonPowerPulse}}$, the test has failed. Otherwise, it has passed.

Table 18 lists the thresholds pertaining to the pass/fail decision of the EA.

Table 18 — Thresholds for the pass/fail decision of the EA

No.	Threshold notation	Meaning of the threshold
1	$T_{\mathrm{RXMonPowerCW}}$	The threshold power at which the injected light monitor indicates an exception event when bright continuous-wave emission is injected into the RX module under test.
2	$T_{\mathrm{RXMonPowerPulse}}$	The threshold peak power at which the injected light monitor indicates an exception event when bright pulsed light emission is injected into the RX module under test.

8.6 EA to test the robustness of the RX module against bright light blinding

8.6.1 General aspects

a) Objective of evaluation activity

This EA intends to test whether the photon detection output of the single-photon detector(s) inside the RX module under test can be controlled by injected bright light. The testing outcome indicates the robustness of the RX module under test against detector blinding attacks, including continuous-wave-light blinding attacks and pulsed-light blinding attacks.

b) Required inputs

The developer shall provide the RX module under test working in the raw data generation stage. The RX module under test shall provide access to the results of measurements performed by the detectors (e.g. digital access to the periods in which detection events were registered in each detector). The dead time duration of each SPD in the RX module under test is known and well characterized.

c) Required tool types and setup

The evaluator shall prepare a tunable laser with a tunable wavelength in the range of $[\lambda_{\mathrm{min}}, \lambda_{\mathrm{max}}]$, this tunable laser should also satisfy the following conditions:

1) It should be able to generate a continuous-wave emission with powers in the range of $[p_{\mathrm{minCW}}, p_{\mathrm{maxCW}}]$.

2) It should also be able to generate laser pulses with peak power in the range of $[p_{\mathrm{minPeak}}, p_{\mathrm{maxPeak}}]$, whose pulse width is in the range of $[w_{\mathrm{min}}, w_{\mathrm{max}}]$, an output repetition frequency that is the same as that of the detectors in the RX module under test and where the arrival time of the pulses can be adjusted over a range of $[d_{\mathrm{min}}, d_{\mathrm{max}}]$ to cover the whole period between the start of adjacent detector gates for a gated detector or the whole period between quantum signals sent from the TX module otherwise. An additional time-delay controller may be used to provide the necessary delay adjustment.

Alternatively, it is possible to use two separate tunable lasers, where one operates in continuous-wave mode with the parameters mentioned in 1) and the other one operates in pulsed mode with the parameters mentioned in 2).

If the TOE adopts a dedicated injected light monitor detecting the laser injection, p_{maxCW} and p_{maxPeak} shall be higher than $T_{\mathrm{RXMonPowerCW}}$ and $T_{\mathrm{RXMonPowerPulse}}$ defined in 8.5 respectively, but lower than power that would destroy components and internal connections.

A laser diode, a state modulator, and a variable attenuator shall be provided to generate optical pulses with pulse energy in the range of $[e_{\mathrm{min}}, T_{\mathrm{trigE}}]$, whose pulse width is in the range of $[w_{\mathrm{minB}}, w_{\mathrm{maxB}}]$.

An optical power meter shall be provided to measure the average energy of the optical pulses with sufficient sensitivity.

The testing tools are connected to the quantum channel interface of the RX module under test. The schematic of the setup for this EA is shown in Figure 19.

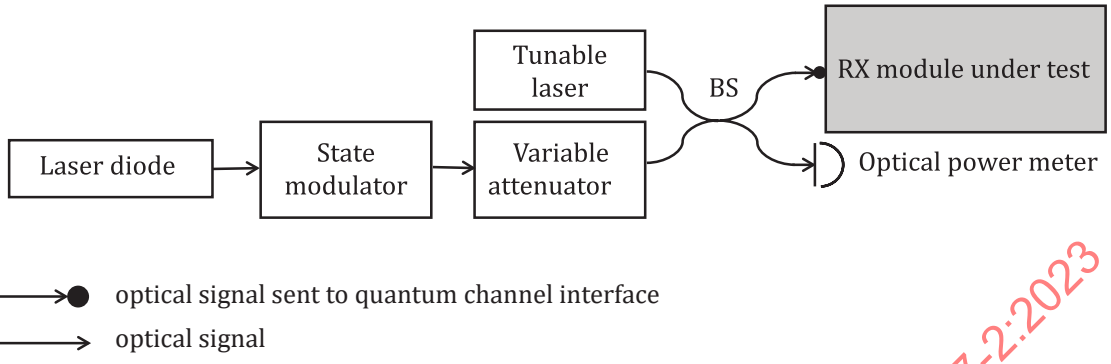


Figure 19 — Schematic of the setup for testing the robustness of the RX module against bright light blinding

d) Rationale

This EA tests the robustness of the RX module under test against bright light injection. The tunable laser can work at the continuous-wave mode (or pulsed mode) to test whether the RX module under test can be blinded by the continuous-wave emission injection (or pulsed laser injection respectively) with different wavelength, power, pulse width and time delay settings (pulse width and time delay settings apply only to pulsed laser). Here, blinding the RX module under test means that there is no detection output during the whole timing period or a period longer than the dead time. The tunable laser can also be operated with a specified maximum power, which limits the highest amount of power an adversary can inject into the RX module under test without destroying components and their internal connections.

After the RX module under test is blinded, the laser diode emits trigger pulses of different power and pulse width, which are modulated into a quantum state required by the QKD protocol to test whether the corresponding detector in the RX module under test can be controlled to output detection results. The verdict that can be given depends on whether RX module under test can be controlled.

8.6.2 Test procedure

In order to simplify the description of the test procedure, the entire procedure is organized as two parts. In detail, the evaluator runs the procedure A to conduct the test, and the steps in procedure A may invoke procedure B to generate trigger pulses and test whether they generate a response.

a) Procedure A

— Step 1: Turn on the RX module under test, and let it work in the raw data generation stage.

— Step 2: Turn on the tunable laser at wavelength $\lambda_{\min}$ and set it to work in the continuous-wave mode.

— Step 3: Set the output power of the tunable laser to be $p_{\min \mathrm{CW}}$. Gradually increase the output laser power until the laser power reaches $p_{\max \mathrm{CW}}$. When increasing the laser power, observe the detection output of the RX module under test over an appropriate acquisition time for each power. For each time without detection output, run the trigger test of procedure B. After all related output powers are tested without the procedure B aborting, go to step 4. Otherwise abort the entire procedure A and report that procedure A failed.

— Step 4: Increase the wavelength by a step of size s_λ, and repeat step 3 until the wavelength reaches $\lambda_{\max}$. After all related wavelengths are tested, proceed to step 5.

— Step 5: Switch the working mode of the tunable laser to pulsed mode and let the tunable laser work at wavelength $\lambda_{\min}$ with minimum peak power p_{minPeak} and minimum pulse width $w_{\min}$. Set the arrival time of laser pulses to be $d_{\min}$.

— Step 6: Gradually increase the peak power of the pulsed laser from the minimum peak power p_{minPeak} until it reaches p_{maxPeak}. For each time when a period of zero detection output is longer than the dead time, run procedure B to do trigger test. After all related peak powers are tested without procedure B aborting, go to Step 7. Otherwise abort the entire procedure A and report that procedure A failed.

— Step 7: Increase the pulse width from $w_{\min}$ by a step of size s_{w}, and repeat step 6 until reaching the maximum pulse width $w_{\max}$. After all related pulse widths are tested, go to step 8.

— Step 8: Gradually delay the time of the optical pulses from $d_{\min}$ to $d_{\max}$ in steps of s_{d} repeating step 7 for each step. $d_{\max}$ and $d_{\min}$ should be at least as long as the period between the start of adjacent detector gates for gated single photon detectors, or at least as long as the period between adjacent signals from the TX module otherwise. After all related delay times are tested, go to step 7.

— Step 9: Increase the wavelength of the laser by a step of size s_{λ} and repeat steps 6 to 8 until the wavelength reaches $\lambda_{\max}$. After all related wavelengths are tested without procedure B aborting, report that procedure A passed.

b) Procedure B

— Step 1: Turn on the laser diode and state modulator to generate trigger pulses with the minimum pulse width w_{minB} with an encoded state arriving at the gate of the corresponding detector in the RX module under test.

— Step 2: Gradually increase the energy of the trigger pulses from the minimum pulse energy $e_{\min}$ until observing the corresponding detection output (the detection output can be deterministic or probabilistic). If no corresponding detection output pulse is observed up to the maximum pulse energy T_{trigE}, go to step 3. Otherwise, abort procedure B.

— Step 3: Increase the pulse width of the trigger pulse by a step of size s_{w}, and repeat step 2 until reaching the maximum pulse width w_{maxB}. If no corresponding photon detection output is observed (the detection output can be deterministic or probabilistic), end procedure B and resume procedure A.

8.6.3 Pass/fail criteria

The test has passed if procedure A reports that it has passed. Otherwise, it has failed.

Table 19 lists the threshold pertaining to the pass/fail decision of the EA.

Table 19 — Threshold for the pass/fail decision of the EA

No.	Threshold notation	Meaning of the threshold
1	T_{trigE}	The threshold pulse energy below which trigger pulses cannot trigger photon detection output in a detector blinding attack.

8.7 EA to test the appropriateness of dead time settings of SPDs

8.7.1 General aspect

a) Objective of the evaluation activity

This EA intends to test whether the raw data generated by the RX module under test excludes any detection events generated during the dead time period of any of the SPDs. The testing outcome indicates whether the TOE is preventing the dead time attack using dead time settings.

b) Required inputs

The developer shall provide the RX module under test working in the raw data generation stage. The RX module under test shall allow the access to the time-tagged digital data. The dead time duration of each SPD in the RX module under test is known and well characterized.

c) Required tool types and setup

The evaluator shall prepare a laser diode followed by a state modulator and a variable attenuator. The state modulator shall be able to randomly modulate the optical pulses to be one of the encoded states used in the QKD protocol under consideration and output the basis choice information. The variable attenuator is capable of attenuating the laser pulses to a constant mean photon number, which is equal to that of a representative quantum state received by the RX module in the raw data generation stage. The variable attenuator is connected to the quantum channel interface of the RX module under test.

The schematic of the setup for performing the EA is shown in Figure 20.

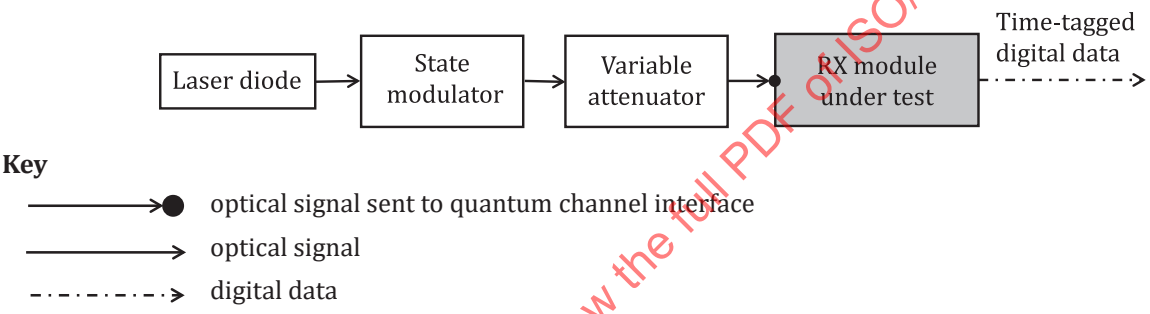


Figure 20 — Setup for testing the appropriateness of dead time settings of SPDs

d) Rationale

This EA tests the implementation of dead time setting for all SPDs. To prevent the RX module under test from the dead time attack, the raw data generated by the RX module under test shall exclude any detection occurring during the dead time period of any of the SPDs.

8.7.2 Test procedure

— Step 1: Turn on the RX module under test, and let it work in the raw data generation stage.

— Step 2: Turn on the laser diode. Adjust the state modulator to randomly modulate the optical pulses as prescribed by the encoding procedure of the implemented QKD protocol. Adjust the variable attenuator to attenuate the laser pulses to a constant mean photon number, which is equal to that of a representative quantum state received by the RX module under test in the raw data generation stage.

— Step 3: Measure a stream of N_{pulse} encoded optical pulses (originating from the laser diode after encoding and attenuation) during an appropriate acquisition time with the RX module under test.

— Step 4: Check the digital data from the RX module, and determine whether there is any time instance at which a detection event is recorded within the relevant dead time. The dead time is after a detection event allowed by the QKD protocol implemented by the RX module under test. Record 0 if any such instances are found and 1 otherwise.

8.7.3 Pass/fail criteria

If step 4 records 1 as a result, the test has passed. Otherwise, it has failed.

There is no threshold pertaining to the pass/fail decision defined in the EA.

8.8 EA to test the temporal profile of the detection efficiency for SPDs

8.8.1 General aspects

a) Objective of the evaluation activity

This EA intends to test if the temporal profile of the detection efficiency when detecting pulses at single-photon level is the same as that when detecting pulses at higher average photon numbers for each SPD. The testing outcome can help determine whether the TOE prevents the after-gate attack, the superlinearity attack, and the avalanche-transition-region attack.

This EA is applicable to RX modules under test that do not have any feedback loop for adjusting the timings of the detectors.

b) Required inputs

The developer shall provide the RX module under test, working in the raw data generation stage. The RX module under test shall allow access to the count rates of the detection events corresponding to each input state measured by the RX module. This means providing access to one count rate for each state at the input from the quantum channel for which the RX module performs measurement(s). One such count rate includes all relevant detection events that are considered by the RX module to be measurements of a particular input state under the QKD protocol.

NOTE Some RX modules change the configuration of the decoding optics over time to alter the detector(s) that a particular input state is intended to be delivered to. Multiple detectors can contribute relevant detection events to the count rate for a particular input state over time. At certain times an RX module can be configured not to contribute relevant detection events in any detector for a particular input state.

c) Required tool types and setup

The evaluator shall prepare a pulsed laser diode followed by the state modulator and a variable attenuator where it is possible to adjust the arrival time of the encoded pulses relative to the timing of measurements within the RX module. The encoded pulses are injected into the quantum channel interface of the RX module under test. The schematic of the setup for performing the EA is shown in Figure 21.

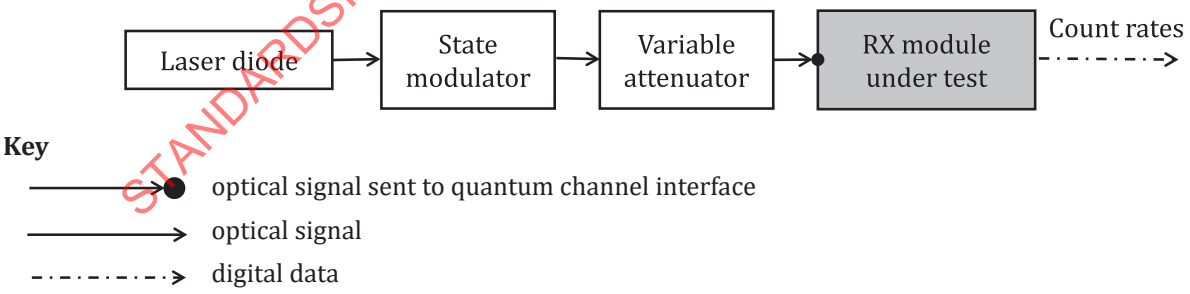


Figure 21 — Setup for testing the temporal profile of the detection efficiency for SPDs

d) Rationale

The EA characterizes the temporal profile of the detection efficiency of the RX module under test for different pulse intensities. The time delay and intensity of the input pulses are adjustable. By comparing the detection window for optical pulses with different intensities, the evaluator can verify

if the temporal profile of the detection efficiency of detecting pulses at a single-photon level is the same as that of detecting pulses at a higher average intensity level for each SPD.

8.8.2 Test procedure

— Step 1: Turn on the RX module under test, and let it work in the raw data generation stage.

— Step 2: Turn on the laser diode. Adjust the state modulator to prepare optical pulses in an encoded state.

— Step 3: Adjust the attenuation of the variable attenuator. Set the intensity of the laser pulses to be a constant mean photon number, which is equal to that of a representative quantum state received by the RX module under test in the raw data generation stage. Send the optical pulses to the RX module under test. The intensity set in this step is constant throughout the entire measurement sequence in step 4.

— Step 4: Adjust the time delay of the encoded pulses and record count rates at each of a set of time delays by accumulating data for some time period, T, for each delay. Characterize the time window over which the SPD detects count rates within the time period, T, that can be resolved above the detector dark counts. Record this range as $[t_{\text{start}}, t_{\text{end}}]$.

— Step 5: Adjust the attenuation of the variable attenuator. Increase the intensity of the optical pulses from $I_{\min}$ to $I_{\max}$ by a step of size s_{I}, where $I_{\min}$ should be higher than the single-photon level. For each intensity I, repeat step 4 and record the SPD detection window range as $[t_{\text{start},I}, t_{\text{end},I}]$.

— Step 6: Calculate the maximum deviation for the start time and end time of the SPD detection window between single-photon level and higher average photon numbers, which are defined according to Formulae (22) and (23):

$$\sigma_{\text{start}} = \max_{I}\{|t_{\text{start}} - t_{\text{start},I}|\} \tag{22}$$

$$\sigma_{\text{end}} = \max_{I}\{|t_{\text{end}} - t_{\text{end},I}|\} \tag{23}$$

where $\max\{\cdot\}$ is the maximum value in a set.

— Step 7: Adjust the state modulator to encode the optical pulses to another state and repeat step 3 to step 6 until all the encoded states are tested. Then repeat step 3 to step 6 for each relevant detector in the RX module under test. Finally, calculate the maximum deviation of the start time and end time of the SPD detection window over all encoded states and relevant detectors as σ_{maxStart} and σ_{maxEnd}.

8.8.3 Pass/fail criteria

If σ_{maxStart} is smaller than the threshold $T_{\text{startTime}}$, and σ_{maxEnd} is smaller than the threshold T_{endTime}, the test has passed. Otherwise, it has failed.

Table 20 lists the thresholds pertaining to the pass/fail decision of the EA.

Table 20 — Thresholds for the pass/fail decision of the EA

No.	Threshold notation	Meaning of the threshold
1	$T_{\text{startTime}}$	The maximum deviation of the start time of a detector gate window when measured with optical signals at a single-photon level and at higher average intensity levels.
2	T_{endTime}	The maximum deviation of the end time of a detector gate window when measured with optical signals at a single-photon level and at higher average intensity levels.

8.9 EA to test the robustness of the RX module against laser injection

8.9.1 General aspects

a) Objective of the evaluation activity

This EA intends to test if the detection probability of the RX module under test can be altered by inserting additional light through the quantum channel interface. The EA checks the response of the RX module under test after it is irradiated by a laser with sufficient power. The test result can be used to verify if the RX module under test prevents the laser damage attack.

This EA is applicable when security is threatened by a mismatch in detection efficiencies of a pair of detectors in the RX module under test.

b) Required inputs

The developer shall provide the RX module under test working in the raw data generation stage. The RX module under test shall allow access to the count rates of detection events corresponding to each input state measured by the RX module. This means providing access to one count rate for each state at the input from the quantum channel for which the RX module performs measurement(s). One such count rate includes all relevant detection events that are considered by the RX module to be measurements of a particular input state under the QKD protocol.

NOTE Some RX modules change the configuration of the decoding optics over time to alter the detector(s) that a particular input state is intended to be delivered to. Multiple detectors can contribute relevant detection events to the count rate for a particular input state over time. At certain times an RX module can be configured not to contribute relevant detection events in any detector for a particular input state.

The developer shall also provide the intrinsic mismatches expected in the count rates for all pairs of measurements on input states that are performed by the RX module under test while receiving input states modulated randomly as prescribed by the encoding procedure of the analysed QKD protocol, but at a constant mean photon number. For example, a QKD protocol may not involve the transmission of or measurement of states with equal probabilities.

c) Required tool types and setup

The evaluator shall prepare a tunable laser followed by a state modulator and an optional optical amplifier that can generate encoded states with powers in the range of $[\,p_{\min}\,,\,p_{\max}\,]$ for a period of T, in order to reach an accumulative effect on the RX module under test according to engineering and evaluation experience. The tunable laser shall also be operated in a wavelength range of $[\,\lambda_{\min}\,,\,\lambda_{\max}\,]$. If the TOE adopts a dedicated injected light monitor to detect bright light, $p_{\max}$ shall be higher than $T_{\mathrm{RXMonPowerPulse}}$ defined in 8.5, but lower than the power that would destroy components and internal connections.

The evaluator shall also provide an optical power meter working in the range of $[\,p_{\min}\,,\,p_{\max}\,]$. A laser diode, a state modulator, and a variable attenuator shall be provided to generate encoded states. The testing tools are connected to the quantum channel interface of the RX module under test. The schematic of the setup for performing the EA is shown in Figure 22.

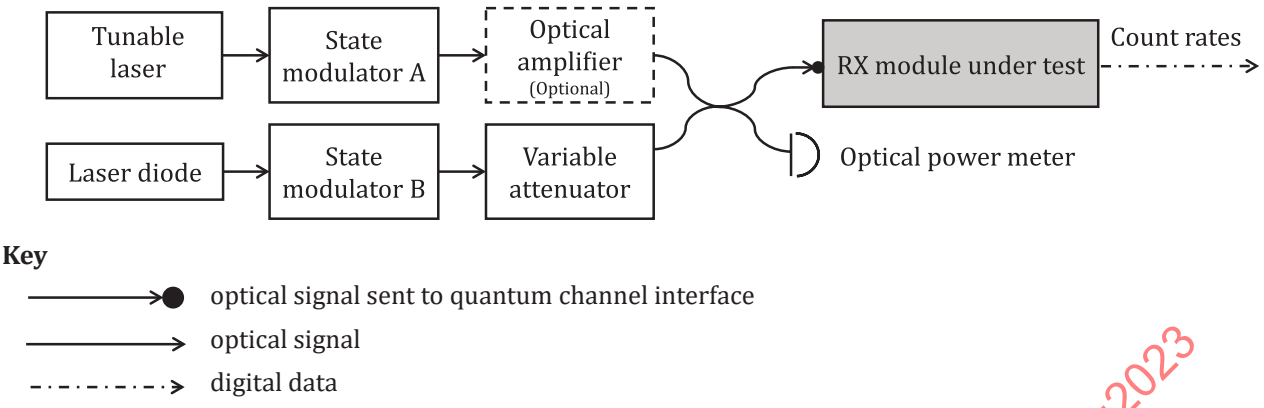


Figure 22 — Schematic of the setup for testing the robustness of the RX module against laser injection

d) Rationale

This EA intends to evaluate the response of the RX module under test after laser irradiation. It seeks to identify cases in which injected light can alter the detection probability of the RX module under test.

This EA describes how to scan each input parameter with a certain step size to test the whole parameter space. However, considering the practical efficiency of conducting the test, these input parameters may be sampled with a random probing method.

e) Dependencies

This EA shall be performed after the EA of 8.2 has been validated.

8.9.2 Test procedure

— Step 1: Turn on the RX module under test, and let it work in the raw data generation stage.

— Step 2: Turn on the tunable laser and optical amplifier (if any) to generate optical pulses with power p_{min} at wavelength λ_{min}.

— Step 3: Set state modulator A to generate an encoded state repeatedly.

— Step 4: Maintain the power for a period T. Then, turn off the tunable laser.

— Step 5: Turn on the laser diode and adjust the state modulator to randomly modulate the optical pulses as prescribed by the encoding procedure of the analysed QKD protocol. Adjust the variable attenuator to attenuate the optical pulses to a constant mean photon number, which is equal to that of a representative quantum state received by the RX module in the raw data generation stage.

Random modulation in this step is optional. Alternatively, the encoded states may be modulated in a representative pattern.

— Step 6: Record for an acquisition time to obtain the count rates output from the RX module under test, denoted by Formula (24)

$$C(p,\lambda,S,i) \tag{24}$$

and Formula (25)

$$C(p,\lambda,S,j) \tag{25}$$

where

i, j are the i-th and j-th outputs respectively from the RX module under test, and $i \neq j$;

p is the power;

λ is the wavelength;

S is the encoded state.

These parameters are the characteristic of the optical pulses that were input from the tunable laser the last time that steps 3 and 4 were performed, i.e. prior to the current acquisition time. This acquisition time shall be long enough that statistical errors in the measurement results are not likely to induce false detection probability mismatches that exceed the threshold.

— Step 7: Turn on the tunable laser at power $p_{\min}$ and wavelength $\lambda_{\min}$. Set state modulator A to repeatedly generate another encoded state. Repeat steps 4 to 6 until all the encoded states are tested.

— Step 8: Turn on the tunable laser to increase the power by a step of size s_p and repeat step 3 to step 7 until the power reaches $p_{\max}$.

— Step 9: Turn on the tunable laser with power $p_{\min}$, and increase the wavelength of the tunable laser by a step of size s_λ. Repeat step 3 to step 8 until the wavelength reaches $\lambda_{\max}$.

— Step 10: Compare all the $C(P,\lambda,S,i)$ and $C(P,\lambda,S,j)$ recorded from all the testing rounds and calculate the maximum mismatch ratio using Formula (26):

$$\sigma_{\text{maxMis}} = \max_{P,\lambda,S,i,j} \left\{ \left| \frac{C(P,\lambda,S,i) - C(P,\lambda,S,j)}{C(P,\lambda,S,i) + C(P,\lambda,S,j)} - \Delta_{i,j} \right| \right\} \tag{26}$$

where

$\Delta_{i,j}$ is the intrinsic mismatch of the detection count rates between the i-th and the j-th outputs from the RX module under test, calculated in a similar manner as the difference of the expected rates divided by the sum for input pulses modulated as expected under the QKD protocol;

NOTE Such intrinsic mismatches typically occur when the QKD protocol implemented involves transmitting and/or performing measurements on each of the encoded states with unequal probabilities.

$\max\{\cdot\}$ is the maximum value in a set.

8.9.3 Pass/fail criteria

If the σ_{maxMis} is smaller than the threshold T_{misRatio}, the test has passed. Otherwise, it has failed.

Table 21 lists the threshold pertaining to the pass/fail decision of the EA.

Table 21 — Threshold for the pass/fail decision of the EA

No.	Threshold notation	Meaning of the threshold
1	T_{misRatio}	The threshold for the maximum tolerable mismatch between the detection probability responses to the laser injection for the RX module under test that are required to be matched under the QKD protocol.

8.10 EA to test the detection limits of homodyne detectors in the RX module

8.10.1 General aspects

a) Objective of the evaluation activity

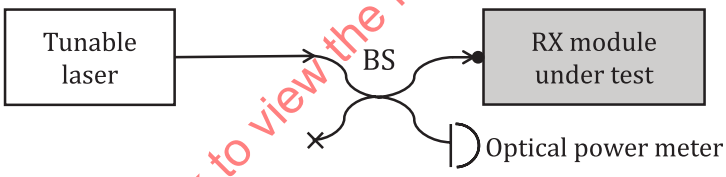
This EA intends to test if an RX module under test rejects the data or reports an exceptional event once the homodyne detector operates in the saturation region. The testing outcome can help verify whether the RX module under test is prevented from the saturation attack and the homodyne blinding attack.

b) Required inputs

The developer shall provide the RX module under test working in the raw data generation stage. At least one of the homodyne detectors inside the RX module under test with stated lower and upper detection limits shall be given. The homodyne detector shall be accessible to light injection and able to be kept unbalanced. Output from the homodyne detector shall be accessible as requested.

c) Required tool types and setup

The evaluator shall provide a tunable laser with output powers in range of $[p_{\min}, p_{\max}]$, and connected to the RX module under test through a BS, where $p_{\min}$ shall be lower than the minimum working power of the homodyne detector, and $p_{\max}$ shall be lower than the power that would destroy components and internal connections. The wavelength of the laser shall be tuned in the working range of the homodyne detector. An optical power meter shall be provided to measure the average energy of the optical pulses with sufficient sensitivity. The testing tools are connected to the quantum channel interface of the RX module under test. The schematic of the setup for performing this EA is shown in Figure 23.



Key

optical signal sent to quantum channel interface

optical signal

Figure 23 — Setup for testing the detection limits of homodyne detectors in the RX module

d) Rationale

This EA validates the linear detection limits of the homodyne detector in the RX module under test. It verifies if the RX module under test accepts abnormal data within the saturation region of the homodyne detector. Here, the saturation region means the homodyne detector operates outside its linear detection region. An adversary can take advantage of the electronic saturation of a homodyne detector to manipulate the noise estimation, which can further lead to a security breach of the TOE. By verifying if the RX module under test abandons data recorded in the saturation region of a homodyne detector, this EA can confirm if the security risk of homodyne detector saturation exists in the RX module under test.

8.10.2 Test procedure

— Step 1: Set the homodyne detector into a testing mode such that the evaluator can obtain measurement results. Configure the homodyne detector to be unbalanced with more light directed to one photodiode than the other.

NOTE To unbalance the homodyne detection, it is possible to simply send optical pulses into the signal port of the homodyne detector since the balance with respect to the local oscillator (LO) port is altered. It is possible that some RX modules provide a procedure to adjust the balance internally while in a testing mode. Another potential alternative is to change the wavelength of the test laser pulses to a value other than the operating wavelength of the TOE (where input filtering in the testing mode permits this).

— Step 2: Set the optical power of the tunable laser to the power p_{min}. Send optical pulses into the RX module under test at the operating frequency of the TOE. Gradually increase the optical power and observe the measurement result from the homodyne detector until the average value is stable. Record the measurement result as γ and the corresponding optical power as p_{stable}.

— Step 3: If γ is a positive value, record it as the value of the upper detection limit, D_{limUp}; if γ is a negative value, record it as the value of the lower detection limit D_{limLow}.

— Step 4: Set the RX module under test in the normal working stage such that it can record data blocks as in the raw data generation stage, but the homodyne detector is kept unbalanced.

— Step 5: Send optical pulses into the homodyne detector with the same working frequency as the TOE. Gradually increase the laser power from the working power to 1,5 times p_{stable} to make sure the homodyne detector reaches its detection limit, and record the data until a whole data block is fulfilled. Check if the RX module under test indicates an exceptional event as a response when the power exceeds p_{stable} and whether the RX module under test rejects the whole data block when such an exceptional event is indicated.

— Step 6: Repeat steps 1 to 5 for other homodyne detector until all detectors in the RX module under test are tested.

8.10.3 Pass/fail criteria

If the RX module under test reports an exceptional event about the homodyne detector saturation and abandons the whole block of data that had been partially or totally recorded outside the range from D_{limLow} to D_{limUp}, the test has passed. Otherwise, it has failed.

There is no threshold pertaining to the pass/fail decision defined in the EA.

8.11 EA to test the appropriateness of double-click event handling

8.11.1 General aspects

a) Objective of the evaluation activity

This EA intends to validate whether the double-click events are appropriately processed in the post-processing stage to avoid security flaws. The testing outcome indicates whether the TOE prevents the double-click attack.

b) Required inputs

This EA is mainly based on documentation review to derive the testing result. The developer shall provide design documents describing how double-click events are processed in the post-processing stage of the RX module under test. In principle, the documentation should include the source code related to the implementation of the mechanism for handling double-click events for high EALs.

c) Required tool types and setup

Since there is no specific testing procedure for this EA, no foreseen setup is specified in this document.

d) Rationale

Double-click events shall be processed appropriately according to the QKD protocol that is being analysed. If these events are directly discarded, the TOE can be vulnerable to the double-click attack.

There exist several valid methods to process double-click events, such as assigning a random bit value to each double-click event.

For generality, this EA does not specify specific testing methods in the test procedure, but it relies on a documentation review method to derive the test result.

As an alternative method, the double-click handling function may be tested by experimentally triggering such events and then validating how the events are handled. However, it is usually inconvenient to realize such tests without adapting the TOE. In such a case, a setup for the testing should be given to indicate the method to induce events and a test procedure should be given to specify the test.

8.11.2 Test procedure

The evaluator shall review the evidence provided by the documentation that describes how double-click events are processed.

8.11.3 Pass/fail criteria

If the documents give sufficient evidence that the double-click events are processed according to a valid method, the test has passed. Otherwise, it has failed.

There is no threshold pertaining to the pass/fail decision defined in the EA.

9 EAs for the evaluation of parameter adjustment procedure(s)

9.1 General

The EAs related to device parameter adjustment procedure are listed in Table 22. These EAs essentially correspond to the security countermeasures applied by the QKD transmitter and receiver modules to resist the known attacks against the device parameter adjustment procedure(s). The general objective of these EAs is to verify the effectiveness of the security countermeasures.

The test procedures described in Clause 9 address known security-related issues of (or attacks against) parameter adjustment procedure that have been published and peer reviewed in academic literature. Although not all have been demonstrated to date, at least one attack strategy has been reported.

The entire TOE should be operated under conditions that are as close to normal operating conditions as possible, which means the security test procedures should be conducted on the TOE as a whole, without requiring additional interfaces, channels, or outputs other than those already present on the TOE. Its objective is to reflect the security status of actual QKD modules under the conditions they can face in operation.

In order to conduct the EM effectively, EAs may allow more modifications to the TOE. Specifically, some of the EAs in Clause 9 require the RX module to provide detection count rates in the output. Alternatively, if necessary, the RX module shall provide the time tagged digital data of the outputs since the detection count rates can be derived from it.

Table 22 — EAs for the parameter adjustment procedure(s)

Evaluation activity	Description	SFRs correspondence	Subclause index	Applicable protocols
Test the inducibility of detection probability mismatch	Test if detection probability mismatch can be induced by tampering with alignment pulses transmitted between the TX module and the RX module under test during the parameter adjustment procedure(s) that performs temporal alignment.	FPT_PHP.3	9.2	DV-PM-QKD; DV-EB-QKD
Test the correctness of shot noise alignment	Test if the shot noise is properly aligned according to the intensity of the local oscillator (LO) in a QKD system.	FPT_PHP.3	9.3	CV-PM-QKD; CV-EB-QKD; CV-MDI-QKD

9.2 EA to test the inducibility of detection probability mismatch

9.2.1 General aspects

a) Objective of the evaluation activity

This EA intends to test if the detection probability mismatch can be induced by tampering with alignment pulses transmitted between the TX module and the RX module under test during the parameter adjustment procedure(s) that performs temporal alignment. The testing outcome indicates whether the TOE prevents attacks against the device alignment procedure(s), which intends to induce detection probability mismatch.

This EA only applies in cases where the TOE includes an alignment procedure that can shift the relative timing of at least a pair of detectors in the RX module under test.

Temporal alignment procedure(s) can adopt different approaches and is dependent upon the protocol(s) used by the TOE, including how states are encoded. The design of the required tampering device should be based on the TOE and the temporal alignment procedures it implements. The test procedure of this EA should be modified to suit the TOE, where necessary.

NOTE In the device alignment procedure attack, the adversary attempts to alter the characteristics of the alignment pulses, such as time delay, wavelength, phase, or polarization, so as to introduce a temporal shift in the detection probability of the SPDs. If such manipulations can induce or increase a detection probability mismatch, it can allow the time-shift attack and the detection-probability-mismatch attack to be launched more efficiently during later QKD sessions. In this EA, only the time delay of the alignment pulses is tested as an example, and if other freedoms are taken into account, the same process can be performed.

b) Required inputs

The developer shall provide an entire TOE that includes a TX module under test and an RX module under test. The TOE shall provide the status of the TOE under test, and the count rates measured by the SPDs in the RX module under test. Where necessary, the TOE may include a test mode in which the evaluator can disable temporal alignments while testing for detector probability mismatch.

c) Required tool types and setup

The evaluator shall prepare a tampering device that is capable of introducing variable delays of up to $d_{\max}$ that are dependent upon the encoded state passing through the tampering device. The design of the tampering device shall be capable of attacking the protocol and the alignment procedure implemented in the TOE. The tampering device shall also be able to switch to a mode in which it can introduce an equal delay to all pulses that pass through it.

Figure 25 shows an example of a potential tampering device for a TOE that uses polarization encoding. It includes optical delay modulators, which can be used to attempt to interfere with the parameter

adjustment procedure that performs temporal alignment. The optical delay modulators are arranged to introduce different relative delays to the alignment optical pulses for different encoded quantum states with some probability. In addition, a bypass containing a single optical delay modulator (not shown) can be included for use in the detection probability mismatch measurements.

The construction of a suitable tampering device can be a complex task. To simplify this task the developer may provide a test mode for the TX module under test in which the tampering device can know the state of each optical alignment pulse sent. The tampering device can then delay each alignment pulse based upon this information. The test mode shall otherwise operate the alignment procedure in the same manner as the normal alignment procedure under test.

The input of the tampering device is connected to the quantum channel interface of the TX module under test, and the output of the tampering device is connected to the quantum channel interface of the RX module under test. The RX module under test shall output the status of the TOE and the count rates, or allow the evaluator to access the information through some evaluation-dedicated interface. The testing scheme is shown in Figure 24.

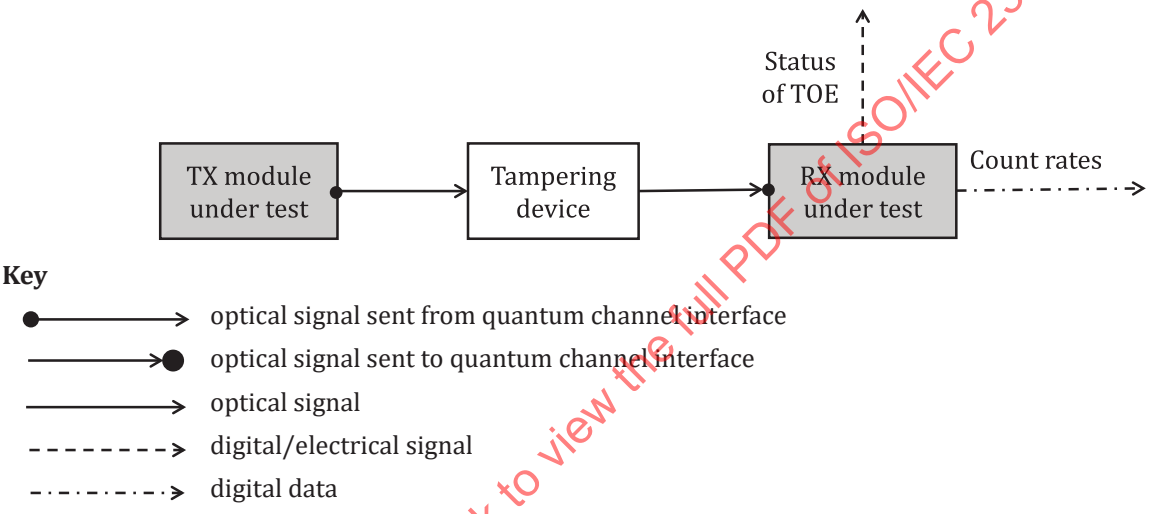
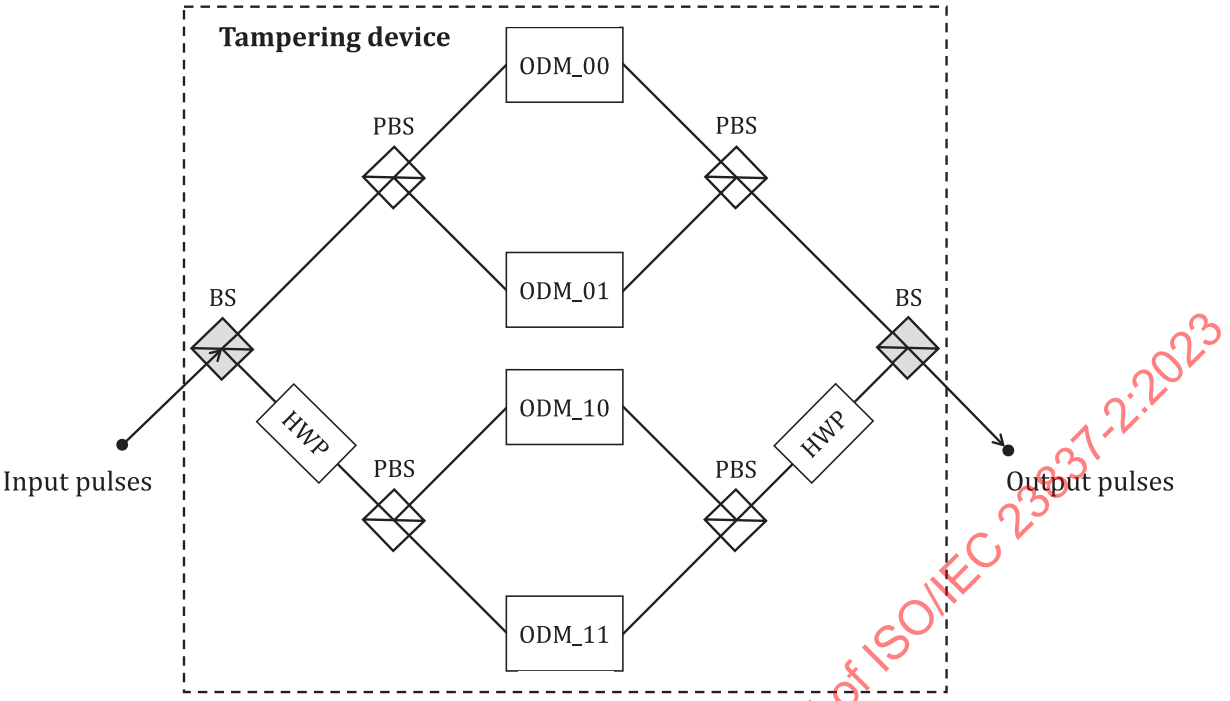


Figure 24 — Setup for testing the inducibility of detection probability mismatch



Key

●⟶	optical signal sent from quantum channel interface
⟶●	optical signal sent to quantum channel interface
⟶	optical signal
PBS	polarizaiton beam splitter
HWP	half-wave plate
ODM	optical delay modulator

Figure 25 — Schematic of a setup for a possible instantiation of tampering device

d) Rationale

This EA intends to test if the detection probability mismatch can be induced by attacks against the device alignment procedure.

During the alignment procedure, the evaluator uses a tampering device to alter the relative delay of the alignment pulses in a manner that is dependent upon their state, with some probability. After the parameter adjustment procedure has concluded, the evaluator checks whether detection probability mismatch has been induced by computing the bit and basis bias of count rates from the RX module as a function of a constant delay applied to all quantum states.

This EA uses of a set of random delays that are kept constant for each single execution of the test. The test is repeated execution times, n_{exe}, to seek a set of delays that can induce a detection probability mismatch. Input parameter, n_{exe}, should be large enough that the EA is statistically likely to have tested sets of delays that include delays in all ranges and combinations that are considered likely to be of interest.

Without loss of generality, the following test procedure is described for QKD protocols that use two basis settings, B_0 and B_1, each with two encoded states. For B_0, the encoded states are S_{00} and S_{01} that encode bit 0 and bit 1, respectively. For B_1, the two encoded states are S_{10} and S_{11} that encode bit

0 and bit 1, respectively. The test procedure may be directly extended for QKD protocols with more basis settings.

e) Dependencies

This EA shall be performed after the function of parameter adjustment procedure(s) has been tested in accordance with 6.4.

9.2.2 Test procedure

— Step 1: Run the TOE to proceed with QKD sessions.

— Step 2: For i from 1 to n_{exe}, run the following steps to compute biases:

a) Randomly choose time delays, d_{00}, d_{01}, d_{10} and d_{11} in the range of 0 to $d_{\max}$, then use the tampering device to set the optical delays for the four states (S_{00}, S_{01}, S_{10}, S_{11}), respectively.

b) Trigger the parameter adjustment procedure of the TOE.

c) Wait for the parameter adjustment procedure to be completed. If the TOE reports an exception and it prevents the system from proceeding to QKD sessions, return to a).

d) Disable further temporal adjustment procedures where necessary.

e) Allow the TOE to proceed with QKD sessions.

f) Switch the tampering device to impose an equal delay to all pulses and set this common delay to d_{minCom}.

g) Record a series of detection events from the RX module under test.

Count the number of times bit 0 and bit 1 that correspond to B_0 occurred, and denote them by N_{00} and N_{01}, respectively. Similarly, count the number of times bit 0 and bit 1 that correspond to B_1 occurred, and denote them by N_{10} and N_{11}, respectively.

Calculate the bit bias in B_0 by using Formula (27)

$$b_0^{(i)} = \max\left\{\left|N_{00}/(N_{00}+N_{01})-1/2\right|, b_0^{(i)}\right\} \tag{27}$$

calculate the bit bias in B_1 with Formula (28)

$$b_1^{(i)} = \max\left\{\left|N_{10}/(N_{10}+N_{11})-1/2\right|, b_1^{(i)}\right\} \tag{28}$$

and calculate the basis bias by using Formula (29)

$$B^{(i)} = \max\left\{\left|N_0/(N_0+N_1)-\Delta\right|, B^{(i)}\right\} \tag{29}$$

where

$N_0 = N_{00} + N_{01}$;

$N_1 = N_{10} + N_{11}$;

Δ is the designed basis ratio of the implemented QKD protocol;

$b_0^{(i)}$, $b_1^{(i)}$, $B^{(i)}$ are set to be 0 before the i-th iteration;

$\max\{\cdot\}$ is the maximum value in a set.

h) Increase the common delay of the tampering device by a step of size, s_d, and repeat the measurement in g) for each delay until reaching maximum common delay, d_{maxCom}. $d_{maxCom} - d_{minCom}$ shall be large enough to cover the full period between states sent by the TX module during QKD sessions.

NOTE For some implementations, it is possible that the parameter adjustment procedure will not stop. In such cases, b) and c) can be aborted after waiting for a defined period of time, and continue the test by going back to step a) as if an exception had been reported.

— Step 3: Compare the derived bit biases, and calculate the maximum delay deviation according to Formulae (30) to (32):

$$b_{max0} = \max_i \left\{ b_0^{(i)} \right\} \tag{30}$$

$$b_{max1} = \max_i \left\{ b_1^{(i)} \right\} \tag{31}$$

$$B_{max} = \max_i \left\{ B^{(i)} \right\} \tag{32}$$

where $\max\{\cdot\}$ is the maximum value in a set.

9.2.3 Pass/fail criteria

For all tested time delays, the test has passed if all of the following conditions are met. Otherwise, it has failed:

a) $b_{max0} < T_{bitBias}$;

b) $b_{max1} < T_{bitBias}$;

c) $B_{max} < T_{basisBias}$.

Table 23 lists the thresholds pertaining to the pass/fail decision of the EA.

Table 23 — Thresholds for the pass/fail decision of the EA

No.	Threshold notation	Meaning of the threshold
1	$T_{basisBias}$	The threshold for the maximum basis bias in the raw data that can be tolerated.
2	$T_{bitBias}$	The threshold for the maximum bit bias in the raw data that can be tolerated.

9.3 EA to test the correctness of shot noise alignment

9.3.1 General aspects

a) Objective of the evaluation activity

This EA intends to test if the shot noise is properly aligned according to the local oscillator (LO) in a TOE. The test measures the shot noise with respect to the local oscillator and indicates whether the TOE uses the proper value of shot noise in its post-processing stage. This EA can check whether the QKD system under test is immune to LO based attacks.

This EA is applicable when the LO is sent from the TX module under test.

b) Required inputs

A developer shall provide an entire TOE that includes a TX module under test and an RX module under test. The TOE shall be able to provide the value of the aligned shot noise as well as the detection efficiency, η', of the homodyne detector. The entire TOE shall be operated in raw data generation stage.

c) Required tool types and setup

The evaluator shall prepare a tampering device, a BS and a calibrated homodyne detector with known detection efficiency η and electronics noise V_{ele}. The tampering device can be either:

— an optical delay modulator, which is used to change the time delay of the optical pulses by at most a time of $d_{\max}$;

— an optical amplifier to increase the optical power of the optical pulses to at most the power, $p_{\max}$;

— a variable attenuator to reduce the optical power of the optical pulses to $p_{\min}$;

— a polarization controller to change the polarization of the optical pulses.

EXAMPLE In practice, the $p_{\min}$ can be 10 % of the LO working power in the TX module under test, and the $p_{\max}$ can be 4 times of the LO working power in the TX module under test.

The quantum channel interface of the TX module under test is connected to the tampering device, while the tampering device is connected to the quantum channel interface of the RX module under test via a BS. The other port of BS is connected to the calibrated homodyne detector. The schematic of the setup for performing the EA is shown in Figure 26.

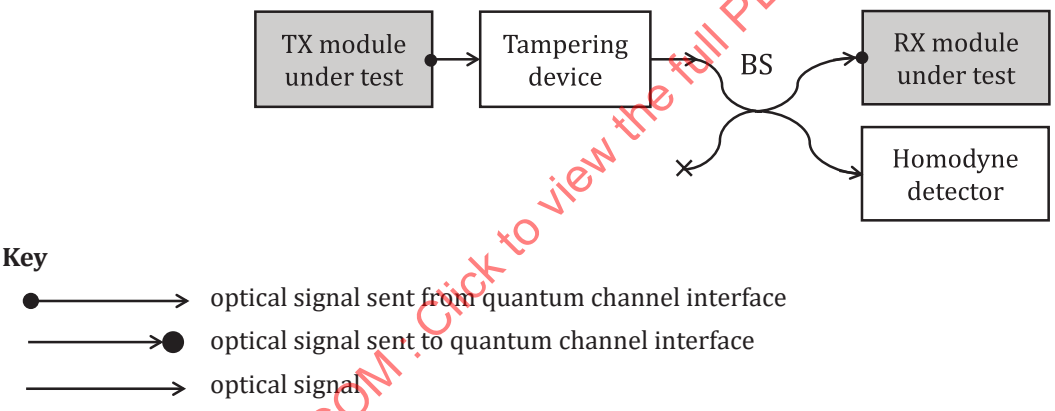


Figure 26 — Schematic of the setup for testing the correctness of shot noise alignment

d) Rationale

This EA intends to test whether the TOE uses and refreshes the shot noise value in the TOE according to the corresponding local oscillator (LO). The tampering device modifies the power, time delay and polarization of LO pulse sent from the TX module, which causes the shot noise change. The evaluation uses a calibrated homodyne detector to measure the shot noise under tampering and compares it with the shot noise value reported in the post-processing procedure of the TOE. It then verifies whether the used shot noise value updates accordingly under the tampering.

9.3.2 Test procedure

— Step 1: Turn on the TX module under test and the RX module under test and let them work in the raw data generation stage.

— Step 2: Use the tampering device to tune the optical delay of LO pulse from 0 to $d_{\max}$ using a step of size, s_{d}. For each time delay:

a) Record $M^{(i)}$ output values of the calibrated homodyne detector and calculate the variance of the $M^{(i)}$ output values, which is denoted by $V^{(i)}$. The shot noise is calculated as Formula (33)

$$V_1^{(i)} = V^{(i)} - V_{\text{ele}} \tag{33}$$

where i denotes the iteration number.

b) Read out the shot noise value from the TOE as $V_1'^{(i)}$. Calculate the shot noise deviation by Formula (34)

$$d_1^{(i)} = \left| \eta V_1'^{(i)} \Big/ \left(\eta' V_1^{(i)} \right) - 1 \right| \tag{34}$$

where

i denotes the iteration number;

η denotes the detection efficiency of calibrated homodyne detector;

η' denotes the detection efficiency of homodyne detector in the TOE.

— Step 3: Calculate the maximum shot noise deviation by Formula (35)

$$D_1 = \max_i \left\{ d_1^{(i)} \right\} \tag{35}$$

where $\max\{\cdot\}$ is the maximum value in a set.

— Step 4: Use the tampering device to tune the optical power of LO pulse from $p_{\min}$ to $p_{\max}$ by a step of size, s_{p}. For each optical power:

a) Record $M^{(j)}$ output values of the calibrated homodyne detector and calculate the variance of the $M^{(j)}$ output values, which is denoted by $V^{(j)}$. The shot noise is calculated as Formula (36)

$$V_2^{(j)} = V^{(j)} - V_{\text{ele}} \tag{36}$$

where j denotes the iteration number;

b) Read out the shot noise value from the TOE as $V_2'^{(j)}$. Calculate the shot noise deviation by Formula (37)

$$d_2^{(j)} = \left| \eta V_2'^{(j)} \Big/ \left(\eta' V_2^{(j)} \right) - 1 \right| \tag{37}$$

where j denotes the iteration number.

— Step 5: Calculate the maximum shot noise deviation by Formula (38)

$$D_2 = \max_j \left\{ d_2^{(j)} \right\} \tag{38}$$

where $\max\{\cdot\}$ is the maximum value in a set.

— Step 6: Use the tampering device to tune the polarization of the LO pulse to be in different directions. For each polarization direction:

a) Record $M^{(k)}$ output values of the calibrated homodyne detector and calculate the variance of the $M^{(k)}$ output values, which is denoted by $V^{(k)}$. The shot noise is calculated as Formula (39)

$$V_3^{(k)} = V^{(k)} - V_{\text{ele}} \tag{39}$$

where k denotes the iteration number;

b) Read out the shot noise value from the TOE as $V_3'^{(k)}$. Calculate the shot noise deviation by Formula (40)

$$d_3^{(k)} = \left| \eta V_3'^{(k)} \Big/ \left(\eta' V_3^{(k)} \right) - 1 \right| \tag{40}$$

where k denotes the iteration number.

— Step 7: Calculate the maximum shot noise deviation by Formula (41)

$$D_3 = \max_k \left\{ d_3^{(k)} \right\} \tag{41}$$

where $\max\{\cdot\}$ is the maximum value in a set.

9.3.3 Pass/fail criteria

If D_1, D_2 and D_3 are all less than the threshold $T_{\text{shotNoise}}$, the test has passed. Otherwise, it has failed.

Table 24 lists the threshold pertaining to the pass/fail decision of the EA.

Table 24 — Threshold for the pass/fail decision of the EA

No.	Threshold notation	Meaning of the threshold
1	$T_{\text{shotNoise}}$	The threshold for the maximum tolerable deviation between the measured shot noise value and the shot noise value adopted in the implementation of the post-processing procedure of the TOE.

10 Supplementary activities for the evaluation of SFRs on conventional network components

10.1 General

A subset of SFRs within the baseline set of SFRs specified in ISO/IEC 23837-1 are related to conventional network components, i.e. those SFRs specified in ISO/IEC 23837-1:2023, 9.2. Functional tests related to conventional network components have already been well documented by the IT evaluation community, the evaluator of QKD modules can thus refer to existing methodologies to perform functional tests. In order to avoid divergence from the existing standardized methods, this document does not specify new EAs to those SFRs, but rather provides general requirements and references to existing standards and specifications in the field.

The general requirements for carrying out EAs for SFRs on conventional network components are summarized as follows, though more specific requirements should be added if needed.

a) General inputs required: This includes firstly the general inputs presented in 5.3.1. For some cases, the TOE is required to be adapted or its test-dedicated functions shall be available such that those tests can be performed. For instance, the randomness test for FCS_RNG.1 requires a direct output from the NRBG component, which typically is not directly accessible to any exterior entity.

b) General tool types required: According to the specific SFRs related to conventional network components, the following should be necessary in performing the relevant evaluation: network sniffer tool, protocol fuzzing tool and crypto-algorithm compliance evaluator.

c) General evaluator competences required: The evaluator for this kind of activities should be an expert in the field of network devices evaluation and have sufficient knowledge about the relevant QKD protocols.

d) General report required: The evaluator shall report the results of functional tests of each EA.

10.2 Evaluation activities for FCS related SFRs overview

The EAs for conventional cryptographic functions have been extensively specified. For QKD modules, conventional cryptographic algorithms and protocols can be applied to protect communications over the key management interface, user authentication, and message authentication over the classical channel. The evaluator is recommended to refer to ISO/IEC 18367 and ISO/IEC 24759 for the compliance test related to FCS_COP.1.

Furthermore, the randomness test for FCS_RNG.1 should refer to relevant methods under an expected EAL, e.g. the method specified in ISO/IEC 20543.

10.3 Evaluation activities for other SFRs overview

For some SFRs within the classes FAU, FDP, FIA, FMT, the common criteria supporting document on evaluation activities for network device cPP[6] gives an appropriate reference for the corresponding EAs. For other SFRs, however, the evaluator is recommended to design new EAs following the community experience on security evaluation of network devices.

11 Supplementary activities for SARs

11.1 General

This clause intends to supplement evaluation activities for the work units of SARs required by the security evaluation of QKD modules. The purpose of the supplementary activities is to provide new requirements to the evaluator, or refine the standardized evaluation activities in ISO/IEC 18045, so as to make the evaluation method for QKD modules completer and more practical. This is realized by emphasizing the characteristics of QKD modules in some work units of SARs.

The following description is organized in alphabetical order of the abbreviated names of the assurance classes defined in ISO/IEC 15408-3. Assurance components and work units without adding supplementary activities are not listed in Table 25 to Table 45, so it is possible that the number in the work unit column of Table 25 to Table 45 is not continuous. The reader is recommended to refer to ISO/IEC 18045 for the complete work units of each SAR.

11.2 Supplementary activities for Class APE: Protection Profile evaluation

The assurance Class APE is designed for the evaluation of PPs. By noting the characteristics of QKD modules, evaluation activities for some work units in APE_INT.1, APE_CCL.1 and APE_SPD.1 are supplemented, see Table 25, Table 26, and Table 27 for detail.

The evaluator shall combine the supplementary content and the standardized content in ISO/IEC 18045 for each work unit to perform the evaluation of PPs on QKD modules.

Table 25 — Supplementary activities for APE_INT.1.1E

Evaluator action element	Work unit	Supplementary activities
APE_INT.1.1E	APE_INT.1–3	The evaluator shall examine the TOE overview to determine that the PP describes the security features of the key establishment function provided by the TOE. The expected communication distance supported by the TOE and the precondition of pre-sharing a secret key for the TOE to work shall also be clearly described.
	APE_INT.1–4	The evaluator shall examine the TOE overview to determine that the TOE type identifies the specific QKD protocol(s) and architecture being implemented in the TOE. The evaluator also identifies the separated TX module(s) and RX module(s), which constitute the TOE for the proper execution of QKD functions [according to the architecture of the implemented QKD protocol(s)].
	APE_INT.1–5	The evaluator shall examine the TOE overview to determine that the external channels and underlying hardware and software platform, such as the chip and operating system, that support the functionality but are excluded from the scope of the TOE, have been identified clearly. In addition, if the TOE implements MDI-QKD or EB-QKD protocols, the evaluator shall examine if the QKD receiver module in MDI-QKD and QKD transmitter module in EB-QKD are clearly excluded from the TOE, or clear explanations have been given to justify the inclusion of these modules otherwise.

Table 26 — Supplementary activities for APE_CCL.1.1E

Evaluator action element	Work unit	Supplementary activities
APE_CCL.1.1E	APE_CCL.1–19	If the conformance statement in the PP under evaluation claims conformance to this document, the evaluator shall examine the conformance statement to determine whether the following statement is included or not: "This PP requires the use of evaluation methods and/or evaluation activities defined in ISO/IEC 23837-2". If included, the evaluator shall demonstrate that the modification of evaluation method/activities (if any) is consistent with and meets the requirements in Clause 12 of this document.
	APE_CCL.1–20 (this is a supplemented unit)	If the PP/ST claims conformance to ISO/IEC 23837-1, the evaluator shall examine the PP/ST to determine that the modification of the security problem definition or SFRs (if any) is consistent with and meets the requirements set in ISO/IEC 23837-1:2023, Clause 10.

Table 27 — Supplementary activities for APE_SPD.1.1E

Evaluator action element	Work unit	Supplementary activities
APE_SPD.1.1E	APE_SPD.1–1	The evaluator shall examine that the security problem definition describes all the identified threats in ISO/IEC 23837-1:2023, Clause 7 with some allowed exceptions as described in ISO/IEC 23837-1:2023, Clause 10. If exceptions are stated, examination of the rationale justification shall be conducted in the work unit of APE_CCL.1–20.

11.3 Supplementary activities for Class ASE: Security Target evaluation

The assurance class ASE is designed for the evaluation of an ST. By noting the characteristics of QKD modules, evaluation activities for some work units in ASE_INT.1 and ASE_TSS.1 are supplemented, which correspond to the evaluation sub-activities of the ST introduction and the TOE summary specification respectively and shall be applied to the security evaluation of STs of QKD modules, as detailed in Table 28 and Table 29.

Table 28 — Supplementary activities for ASE_INT.1.1E

Evaluator action element	Work unit	Supplementary activities
ASE_INT.1.1E	ASE_INT.1–5	The evaluator shall examine the TOE overview to determine that the ST describes the security features of the key establishment function provided by the TOE, including the expected communication distance. The precondition of pre-sharing secret key for the TOE to work shall also be clearly described.
	ASE_INT.1–6	The evaluator shall examine the TOE overview to determine that the TOE type identifies the specific QKD protocol(s) and architecture being implemented in the TOE. The evaluator also identifies the separated TX module(s) and RX module(s) which constitute the TOE for the proper execution of QKD functions [according to the architecture of the implemented QKD protocol(s)].
	ASE_INT.1–8	The evaluator shall examine the TOE overview to determine that the external channels (such as the quantum channel and classical channel) and the underlying hardware and software platform (such as the chip and operating system), which support the functionality but are excluded from the scope of the TOE, have been identified clearly. In addition, if the TOE implements MDI-QKD or EB-QKD protocol(s), the evaluator shall examine whether the QKD receiver module in MDI-QKD and QKD transmitter module in EB-QKD are clearly excluded from the TOE, or whether a clear explanation is given to justify the inclusion of these modules.
	ASE_INT.1–10	The evaluator shall examine the TOE overview to determine that the TOE includes the modules required by the implemented QKD protocols. It shall be clearly stated that some modules are regarded as non-TOE parts where relevant, such as the QKD receiver module in MDI-QKD and QKD transmitter module in EB-QKD.

Table 29 — Supplementary activities for ASE_TSS.1.1E

Evaluator action element	Work unit	Supplementary activities
ASE_TSS.1.1E	ASE_TSS.1–1	The evaluator shall examine the TSS to determine that it describes the IT-related controls used by the TOE to meet the security objective, especially those controls used to resist side channel attacks from the quantum channel interface.

11.4 Supplementary activities for Class ADV: Development

11.4.1 Supplementary activities for ADV_ARC

The objective of this activity is to determine whether the TSF is structured such that it cannot be tampered with or bypassed, and whether TSFs that provide security domains isolate those domains

from each other. Some supplementary activities are given by noting the characteristics of QKD modules, as shown in Table 30.

Table 30 — Supplementary activities for ADV_ ARC.1.1E

Evaluator action element	Work unit	Supplementary activities
ADV_ARC.1.1.E	ADV_ ARC.1–1	None.
	ADV_ ARC.1–2	The evaluator shall examine the security architecture description to determine that the system process space and memory sections for post-processing procedure and final key (and relevant keying material) are separated from the system process space and memory sections, such that the access to the final key and relevant keying material is constrained by system access control measures.
	ADV_ ARC.1–3	The evaluator shall examine the security architecture description to determine that in the initialization stage, the TOE does not perform QKD sessions until the system parameters have been successfully aligned and the system has achieved a stable state.
	ADV_ ARC.1–4	The evaluator shall examine the security architecture description to determine that all the known active side channel attacks from the quantum channel have been considered and addressed, such that the TSF is able to protect itself from physical tampering attacks.
	ADV_ ARC.1–5	The evaluator shall examine the security architecture description to determine that all the test-purpose interfaces are closed or limited, and all the known passive side channel attacks from the quantum channel have been considered and addressed, such that SFR-enforcing mechanisms cannot be bypassed.

11.4.2 Supplementary activities for ADV_FSP

The objective of this activity is to determine whether the developer has provided a high-level description of TSFIs. Some supplementary activities are provided by noting the characteristics of QKD modules, shown in tables from Table 31 to Table 35.

Table 31 — Supplementary activities for ADV_FSP.1.1E

Evaluator action element	Work unit	Supplementary activities
ADV_FSP.1.1E	ADV_FSP.1–1	The evaluator shall examine the functional specification to determine that the purpose of the external interfaces of the QKD modules has been clearly stated. In particular, the control and management interface may be implemented by a set of specific interfaces, which are designed for different aspects of the system control and management function, and instantiated by different physical ports, such as USB port, network port. The FSP document provides a place for the developer to clearly describe these interfaces.

Table 32 — Supplementary activities for ADV_FSP.2.1E

Evaluator action element	Work unit	Supplementary activities
ADV_FSP.2.1E	ADV_ FSP.2–2	The evaluator shall examine the functional specification to determine that the purpose of the external interfaces of the QKD modules has been clearly stated. In particular, the control and management interface may be implemented by a set of specific interfaces, which are designed for different aspects of the system control and management function, and instantiated by different physical ports, such as USB port, network port. The FSP document provides a place for the developer to clearly describe these interfaces.

Table 33 — Supplementary activities for ADV_FSP.3.1E

Evaluator action element	Work unit	Supplementary activities
ADV_FSP.3.1E	ADV_FSP.3–2	The evaluator shall examine the functional specification to determine that the purpose of the external interfaces of the QKD modules has been clearly stated. In particular, the control and management interface may be implemented by a set of specific interfaces, which are designed for different aspects of the system control and management function, and instantiated by different physical ports, such as USB port, network port. The FSP document provides a place for the developer to clearly describe these interfaces.

Table 34 — Supplementary activities for ADV_FSP.4.1E

Evaluator action element	Work unit	Supplementary activities
ADV_FSP.4.1E	ADV_FSP.4–2	The evaluator shall examine the functional specification to determine that the purpose of the external interfaces of the QKD modules has been clearly stated. In particular, the control and management interface may be implemented by a set of specific interfaces, which are designed for different aspects of the system control and management function, and instantiated by different physical ports, such as USB port, network port. The FSP document provides a place for the developer to clearly describe these interfaces.

Table 35 — Supplementary activities for ADV_FSP.5.1E

Evaluator action element	Work unit	Supplementary activities
ADV_FSP.5.1E	ADV_FSP.5–3	The evaluator shall examine the functional specification to determine that the purposes of the external interfaces of the QKD modules have been clearly stated. In particular, the control and management interface may be implemented by a set of specific interfaces, which are designed for different aspects of the system control and management function, and instantiated by different physical ports, such as USB port, network port. The FSP document provides a place for the developer to clearly describe these interfaces.

11.5 Supplementary activities for Class AGD: Guidance documents

11.5.1 Supplementary activities for AGD_OPE

The objectives of this activity are to determine whether the user guidance describes the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and

detection of insecure TOE states, or whether it is misleading or unreasonable. Supplementary activities are given in Table 36.

Table 36 — Supplementary activities for AGD_OPE.1.1E

Evaluator action element	Work unit	Supplementary activities
AGD_OPE.1.1E	AGD_OPE.1–3	The evaluator shall examine the operational user guidance to determine that system security parameters under the control of the operator and their default values have been clearly described. Since these parameters may be changed by the operator, the description of the parameters should identify reasonable values for the secure operation of the TOE.
	AGD_OPE.1–5	The evaluator shall examine the operational user guidance to determine that the guidance identifies all possible modes of operation of the system (including failure and normal operation modes) and the methods to distinguish the models from the appearance of the TOE (e.g. signal lights), such that the operator can adopt measures in time in case of emergency incidents.

11.5.2 Supplementary activities for AGD_PRE

The objective of this activity is to determine whether the procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Supplementary activities are given in Table 37.

Table 37 — Supplementary activities for AGD_PRE.1.1E

Evaluator action element	Work unit	Supplementary activities
AGD_PRE.1.1E	AGD_PRE.1–2	The evaluator shall examine the provided installation procedures to determine that the steps necessary for secure deployment of the TOE and the secure preparation of the operational environment are described, so as to validate whether the assumptions set on the operational environment can be satisfied.

11.6 Supplementary activities for Class ATE: Test

11.6.1 Supplementary activities for ATE_FUN

Functional testing performed by the developer provides assurance that the tests in the test documentation are performed and documented correctly. The family ATE_FUN contributes to providing assurance that the likelihood of undiscovered flaws is relatively small. The supplementary activities for ATE_FUN are listed in Table 38.

Table 38 — Supplementary activities for ATE_FUN.1

Evaluator action element	Work unit	Supplementary activities
ATE_FUN.1.1E	ATE_FUN.1–2	The evaluator shall examine the test plan to determine that it describes the information on test equipment and special preparation of the TOE. Some EAs for these aspects require special preparation of the TOE in order to get the intermediates of the execution or facilitate the setup of a testing environment. The developer is thus required to clearly describe the test configuration.
	ATE_FUN.1–4	Regarding the evaluation of EAs, the evaluator shall examine the test plan to determine that the dependencies of EAs are considered in the functional testing. This should be consistent with the dependencies item of each EA described in Clause 6 to Clause 9, or any other dependency relationships that are arguably reasonable.
	ATE_FUN.1–5	Regarding the evaluation of EAs, the evaluator shall examine the test documentation to determine that all expected test results are consistent with the threshold values predefined in the ST or relevant documents for the evaluation.
	ATE_FUN.1–6	Regarding the evaluation of EAs, the evaluator shall check that the actual pass/fail verdicts in the test documentation are consistent with the pass/fail criteria in this document or other relevant documents for the evaluation.

11.6.2 Supplementary activities for ATE_IND

The family ATE_IND deals with the degree to which there is independent functional testing of the TSF. Activities related to the family include verifying the developer testing and performing additional tests. Supplementary activities for the work units in the activity actions ATE_IND.1 and ATE_IND.2 are listed in Table 39 and Table 40 respectively.

Table 39 — Supplementary activities for ATE_IND.1

Evaluator action element	Work unit	Supplementary activities
ATE_IND.1.1E	ATE_IND.1–1	The evaluator shall examine the TOE to determine that the test configuration and the special preparation of the TOE are suitable for the testing of QKD protocol implementation, quantum optical components and parameter adjustment procedure(s). This is based on the requirements that the TOE may need some modifications to facilitate the setup of the evaluation environment of EAs.
ATE_IND.1.2E	ATE_IND.1–3	Regarding the evaluation of EAs, the evaluator shall incorporate the EAs specified in Clause 6 to Clause 9 into the devised test subset if the actually adopted evaluation methods are claimed to be compliant with this document (with some allowed exceptions described in Clause 12).
	ATE_IND.1–7	Regarding the evaluation of EAs, the evaluator shall check whether the actual test result is consistent with the threshold values predefined in the ST and/or relevant documents for the evaluation, if the actually adopted evaluation methods are claimed to be compliant with this document (with some allowed exceptions described in Clause 12).