Supporting Document

Mandatory Technical Document

Evaluation Method for Protection Profile for Prepare and Measure Quantum Key Distribution Modules

May 2025

Version 1.0 EnJp

Reference

QF-TD-QKD-2025-002_SDv1.0_EnJp

Disclaimer

The present document has been produced and approved by the Quantum Key Distribution Technology Promotion Committee and represents the views of those members who participated in this committee.
It does not necessarily represent the views of the entire Quantum Forum membership.

Copyright Notification

Acknowledgement

（本ページ和訳省略）

This work was partly supported by the following national projects:
“Research and Development for Construction of a Global Quantum Cryptography Network (JPJ008957)” in “R&D of ICT Priority Technology (JPMI00316)” of Ministry of Internal Affairs and Communication (MIC), Japan.; and
Council for Science, Technology and Innovation (CSTI), Cross-ministerial Strategic Innovation Promotion Program (SIP), “Photonics and Quantum Technology for Society 5.0” (Funding agency: QST).

Sincere gratitude is extended to the members of European Telecommunications Standards Institute (ETSI), Industry Specification Group on Quantum Key Distribution (ISG-QKD) for their insightful discussions on this document.

Authors

Masato Koashi
University of Tokyo
Akihisa Tomita
Hokkaido University
Go Kato
National Institute of Information and Communications Technology
Mikio Fujiwara
National Institute of Information and Communications Technology
Masahide Sasaki
National Institute of Information and Communications Technology
Ken-ichiro Yoshino
NEC Corporation
Shinya Hirashita
NEC Corporation
Yoshimichi Tanizawa
Toshiba Corporation
Akira Murakami
Toshiba Digital Solutions Corporation
Kenji Yamaya
ECSEC Laboratory Inc.

Reviewers: *QKD Technical Review Committee*

Kiyoshi Tamaki, Chair
University of Toyama
Toyohiro Tsurumaru, Vice chair
Mitsubishi Electric Corporation
Toshimori Honjo
Nippon Telegraph and Telephone Corporation
Kaoru Kenyoshi
National Institute of Information and Communications Technology
Ryutaroh Matsumoto
Institute of Science Tokyo
Takao Saito
ECSEC Laboratory Inc.

Foreword

This is a Supporting Document (SD), intended to complement the Common Criteria (CC) 2022, Revision 1 and the associated Common Evaluation Methodology for Information Technology Security Evaluation (CEM).

これは、コモンクライテリア（CC）2022 版、改訂 1 版及び関連する情報技術セキュリティ評価共通評価手法（CEM）を補完することを意図したサポート文書（SD）である。

Supporting documents may be “Guidance Documents”, that highlight specific approaches and application of the standard to areas where no mutual recognition of its application is required, and as such, are not of normative nature, or “Mandatory Technical Documents”, whose application is mandatory for evaluations whose scope is covered by that of the supporting document. The usage of the latter class is not only mandatory, but certificates issued as a result of their application are recognized under the Common Criteria Recognition Arrangement (CCRA). This SD shall be considered a Mandatory Technical Document.

サポート文書は、規格の適用に関する相互承認が要求されない分野への特定のアプローチと適用を強調する「ガイダンス文書」であり、そのようなものとして規範的な性質を持たないものである場合と、サポート文書の適用範囲に含まれる評価への適用が必須である「必須技術文書」である場合がある。後者のクラスは、使用が義務付けられているだけでなく、その適用結果として発行された認証書は、CC 相互承認アレンジメント（CCRA）の下で承認される。本 SD は、必須技術文書とみなされる。

Conventions

Citations from CC and CEM are indicated by square brackets.

CC および CEM からの引用は四角囲みで表す。

Document titles and citations are shown in *italics*.

文書のタイトルや引用は*斜体*で表す。

Terminology

Glossary

For definitions of standard CC terminology see [CC] part 1.

Term	Meaning
ADV	Assurance class: Development
AGD	Assurance class: Guidance Documents
ASE	Assurance class: Security Target
ATE	Assurance class: Test

Term	Meaning
AVA	Assurance class: Vulnerability Assessment

Acronyms

Acronym	Meaning
BB84	Bennett-Brassard 84 Protocol
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CV-QKD	Continuous-Variable Quantum Key Distribution
DSC	Dedicated Security Component
DV-QKD	Discrete Variable Quantum Key Distribution
EA	Evaluation Activity
EAL	Evaluation Assurance Level
EB-QKD	Entanglement-Based Quantum Key Distribution
HCD	Hard Copy Device
PP	Protection Profile
QKD	Quantum Key Distribution
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SD	Supporting Document
ST	Security Target
TOE	Target Of Evaluation
TSF	TOE Security Functionality
TSFI	TOE Security Functional Interface

References

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; November 2022, CC:2022, Revision 1, CCMB-2022-11-001

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; November 2022, CC:2022, Revision 1, CCMB-2022-11-002

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements; November 2022, CC:2022, Revision 1, CCMB-2022-11-003

[CC4] Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities; November 2022, CC:2022, Revision 1, CCMB-2022-11-004

[CC5] Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements; November 2022, CC:2022, Revision 1, CCMB-2022-11-005

[CCEI] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), 002, Version 1.1, February 1, 2024

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, November 2022, CEM:2022 Revision 1, CCMB-2022-11-006

[ISO/IEC 23837-2] ISO/IEC 23837-2:2023 Information security—Security requirements, test and evaluation methods for quantum key distribution—Part 2: Test and evaluation methods, Edition 1, 2023

[ETSISP] STABLE DRAFT Title: Quantum Key Distribution; Security Proofs, ETSI GS QKD 005 V1.3.2 (2021-03)

[AIS20/31] A proposal for: Functionality classes for random number generators, Version 2.0, 18 September 2011

[SP800-22] A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, Revision 1a, April 2010

[PP-EAL4] Common Criteria Protection - Profile Pair of Prepare and Measure Quantum Key Distribution Modules, ETSI GS QKD 016 V2.1.1 (2024-01)

[PP-EAL2] Prepare and Measure Quantum Key Distribution Modules Protection Profile, Version 1.00

[DSCSD] Supporting Document: Evaluation Activities for collaborative Protection Profile for Dedicated Security Component: Mandatory Technical Document, Version 2.0, October 28, 2024

[HCDSD] Supporting Document Mandatory Technical Document Evaluation Activities for collaborative Protection Profile for Hardcopy Devices Version 1.0e, 4 March 2024

[NDSD] Evaluation Activities for Network Device cPP Version: 3.0e Date: 06-December-2023

Table of Contents

1. Evaluation method introduction

1.1. Evaluation method identifier

Title: Supporting Document Mandatory Technical Document Evaluation Method for Protection Profile for Prepare and Measure Quantum Key Distribution Modules

Version: 1.0 EnJp

Date: May 2025

1.2. Entity responsible for the evaluation method

Quantum Key Distribution Technology Promotion Committee, Quantum Forum

量子フォーラム 量子鍵配送技術推進委員会

1.3. Technology area and scope of supporting document

This document defines the refinements of SARs and evaluation activities for Quantum Key Distribution (QKD) protocol implementation evaluation in accordance with Common Criteria. Currently, this document supports only the decoy-state BB84 protocol (which is one of the DV-QKD protocols). This document further focuses on a specific implementation called time-bin encoding, in which a pair of optical pulses are transmitted in each of the repeated rounds of communication. In some sections, however, other encoding schemes will be mentioned in the context of discussing general issues in QKD, such as vulnerability analysis. The QKD protocol is a security functional requirement of the PP/ST for QKD modules and is implemented in the QKD module. This document provides evaluation method for the QKD protocol implementation. Other security functions implemented in the QKD module shall be evaluated based on SARs in [CC], [CEM] and other supporting documents.

この文書は、コモンクライテリアに従った量子鍵配送（QKD）プロトコル実装の評価のための SAR の詳細化、及び、評価アクティビティを定義する。現在、この文書でサポートされている QKD プロトコルは、“Decoy-state BB84 with time-bin encoding”（DV-QKD の 1 つ）のみである。本書ではさらに、タイムビンエンコーディングと呼ばれる、繰り返される通信の各ラウンドで一対の光パルスが送信される特定の実装に焦点を当てる。しかし、一部のセクションでは、耐タンパ性分析などの QKD に関する一般的な問題を論じる文脈において、他のエンコーディング方式についても言及する。QKD プロトコルは QKD モジュールの PP/ST のセキュリティ機能要件であり、QKD モジュールに実装される。この文書は、QKD プロトコル実装の為の評価方法を提供する。QKD モジュールに実装されている他のセキュリティ機能は、[CC]の SAR および[CEM]、他のサポート文書に基づいて評価されなければならない。

1.4. Evaluation method overview

1.4.1. PP Reference

This document refers to [PP-EAL4] and [PP-EAL2].

この文書は、[PP-EAL4]と[PP-EAL2]を参照する。

This document may be applied to the CC evaluation of TOEs claiming to comply with one of the above PPs. The developer and the evaluator shall select the content and presentation elements of the required developer evidence

and work units that correspond to the assurance components in the assurance package of the compliant PP. Table 1-1 shows the corresponding content and presentation elements and work units to be selected for each PP. In other words, when evaluating the TOE that conforms to [PP-EAL2], refer to the left column of Table 1-1, and when evaluating the TOE conforms to [PP-EAL4], refer to the right column of Table 1-1.
The content and presentation elements of the required developer evidence are detailed in Section 3. Evaluation activities of work units are defined in Section 8.
この文書は、上記の PP のいずれかに適合していると主張する TOE の CC 評価に適用できる。
開発者及び評価者は、要求される開発者エビデンスの内容及び提示エレメント、並びに適合 PP の保証パッケージの保証コンポーネントに対応するワークユニットを選択しなければならない。Table 1-1 に、各 PP で選択すべき対応する内容及び提示エレメント、ワークユニットを示す。つまり、[PP-EAL2]に適合した TOE の評価においては、Table 1-1 の左側の列を参照し、[PP-EAL4]に適合した TOE の評価においては、Table 1-1 の右側の列を参照する。
要求される開発者エビデンスの内容及び提示エレメントは、3 章に詳述する。ワークユニットの評価アクティビティは、8 章に定義されている。

Table 1-1 Correspondence between the PPs and content and the presentation elements and the work units

[PP-EAL2]	[PP-EAL4]
Content and presentation elements in Section 3: Required inputs	
ADV_FSP.2.1C	ADV_FSP.4.1C
ADV_FSP.2.3C	ADV_FSP.4.3C
ADV_ARC.1.2C	
ADV_ARC.1.4C	
ADV_ARC.1.5C	
AGD_OPE.1.3C	
AGD_OPE.1.5C	
ATE_COV.1.1C	ATE_COV.2.2C
ATE_FUN.1.1C	
Work units in Section 8 Evaluation activities	
ASE_REQ.2-11	
ADV_ARC.1-2	
ADV_ARC.1-4	
ADV_ARC.1-5	
ADV_FSP.2-4	ADV_FSP.4-5
ADV_FSP.2-5	ADV_FSP.4-6
ADV_FSP.2-9	ADV_FSP.4-11
ADV_FSP.2-10	ADV_FSP.4-12
ADV_TDS.1-7	ADV_TDS.3-15
ADV_TDS.1-8	ADV_TDS.3-16
AGD_OPE.1-3	
AGD_OPE.1-5	
ATE_COV.1-1	ATE_COV.2-4
ATE_FUN.1-1	

[PP-EAL2]	[PP-EAL4]
AVA_VAN.2-3	AVA_VAN.5-3

The two PPs define equivalent functional requirements, but some SFR identifications are different. The correspondence between their SFR identifications is detailed in Table 1-2. The functional tests for SFRs defined in [PP-EAL2] are described in Section 10.
2 つの PP は同等の機能要件を定義しているが、一部の SFR 識別が異なっている。それぞれの SFR 識別の対応を Table 1-2 に示す。[PP-EAL2]に定義されている SFR の機能テストが 10 章に記述されている。

Table 1-2 Correspondence of SFR identifications

[PP-EAL2]	[PP-EAL4]
FCS_QKD.1	
FPT_ITQ.1	FPT_ITC.1
FPT_EMS.1	
FPT_PHP.3	
FPT_FLS.1	FPT_FLS.1/Fail FPT_FLS.1/EoL
FCS_CKM.6	FCS_CKM.6/EXP FCS_CKM.6/QAK
FCS_COP.1	FCS_COP.1/CCI
FCS_RNG.1	

1.4.2. Concept of the evaluation for the QKD protocol implementation

The security of QKD protocols is mathematically proven as information-theoretical security, meaning that the keys exchanged are secure against attackers who have unbounded computing resources. Security proofs demonstrate that a QKD protocol remains secure under assumptions on the characteristics of the devices used in the QKD system and the conditions on processing in the QKD protocol. Security proofs should preferably take imperfections of the QKD system into account. Unfortunately, however, such security proofs rely on highly precise device characterization techniques, which still require further research and development. Therefore, it is often the case that most assumptions represent perfect devices and the ideal conditions on processing. In this document, such representations are referred to as assumptions of “ideal characteristics”. On the other hand, assumptions that represent realistic devices and practical conditions on processing are referred to as assumptions of “realistic characteristics”.
Each assumption of ideal characteristics is usually simpler in its description compared to a corresponding assumption of realistic characteristics. It is likely that security proofs taking into account realistic device characteristics and practical processing conditions would require more assumptions than those based on ideal characteristics. Therefore, it would be reasonable to recognize that each assumption of ideal characteristics defines an “assumption family”, and each family may include one or more assumptions of realistic characteristics. For the QKD protocol implemented in the TOE, the assumptions in security proofs (whether ideal or realistic) are not always completely fulfilled, and there are deviations between the assumptions and the corresponding characteristics to them in the implementation of the TOE, referred to as “implementation characteristics”. Such deviations may

compromise the implemented QKD protocol and should be treated as potential vulnerabilities in the QKD protocol. Note that the requirements in the PPs and the assumptions in security proofs are different. The requirements in the PPs are unconditionally fulfilled for any TOE to pass the evaluation, but the assumptions in security proofs are not fulfilled in some cases.
To conduct vulnerability analysis and testing upon the TOE, it is often necessary to restate, modify, or relax the assumptions in security proofs to be testable and preferably quantitative in terms of physical parameters or characteristics rather than remaining in strict and abstract descriptions that current technology cannot implement. This document addresses the assumptions commonly used in security proofs of many QKD protocols, whose concrete descriptions are provided in Section 9 and considers their corresponding testable physical parameters or characteristics, hereafter referred to as “testable parameters/characteristics”. In Section 3, commonly used assumption families are listed in Table 3-1, and the testable parameters/characteristics are mapped to each family. Functional tests are derived in Section 10. When designing the functional tests and determining pass/fail criteria, it is often considered that the achievable key generation rate should be practically relevant and not unnecessarily restricted by the criteria of the functional tests.
The testable parameters/characteristics mapped to the assumptions in the security proofs can be linked to appropriate functional test(s) in Section 10.
Regarding parameters/characteristics that are not tested, the developer shall create and provide the guidance to the TOE user to ensure that the performance of TOE components related to those parameters/characteristics are adequately maintained.

QKD プロトコルの安全性は、情報理論的安全性として数学的に証明されている。これは、交換される鍵が、無制限の計算資源を持つ攻撃者に対して安全であることを意味する。セキュリティ証明は、QKD システムで使用されるデバイスの特性や QKD プロトコルの処理条件に関する仮定の下で、QKD プロトコルが安全であることを示すものである。セキュリティ証明は、QKD システムの不完全性を考慮することが望ましい。しかし残念ながら、このようなセキュリティ証明は、非常に精密なデバイス特性評価技術に依存しており、さらなる研究と開発が必要とされている。そのため、多くの仮定は完全な装置と処理上の理想的な条件を表すことが多い。本書では、このような表現を「理想的な特性」の仮定と呼ぶ。一方、現実的な装置や現実的な処理条件を表す仮定を「現実的特性」の仮定と呼ぶ。
TOE に実装された QKD プロトコルでは、（理想的であれ現実的であれ）セキュリティ証明の仮定が常に完全に満たされるとは限らず、仮定とそれに対応する TOE の実装における特性（「実装特性」と呼ばれる）との間にずれが存在する。このようなずれは、実装された QKD プロトコルを危うくする可能性があり、QKD プロトコルの潜在的な脆弱性として扱われるべきである。 PP における要求事項とセキュリティ証明における仮定は異なることに注意すること。PP の要求事項は、評価に合格するどのような TOE に対しても無条件に満たされるものである。
TOE の脆弱性分析とテストを実施するためには、多くの場合、現在の技術では実装できないような厳密で抽象的な記述のままではなく、物理的なパラメータや特性の観点からテスト可能で、できれば定量的であるように、セキュリティ証明の仮定を再表現、修正、または緩和する必要がある。この文書では、多くの QKD プロトコルのセキュリティ証明で一般的に使用される仮定を取り上げ、その具体的な定義を 9 章で提供し、それらに対応するテスト可能な物理的パラメータまたは特性（以下「テスト可能なパラメータ／特性」という）を考える。3 章では、一般的に使用される仮定ファミリを Table 3-1 にリスト化し、テスト可能なパラメータ／特性をそれぞれのファミリにマッピングする。機能テストは 10 章で導出される。機能テストを設計し、合否判定基準を決定する際、達成可能な鍵生成速度が実用上意味あるものとなるよう、そして、機能テストの基準によって不必要に制

限される事のないように留意する。
セキュリティ証明の仮定に対応付けられたテスト可能なパラメータ／特性は、10 章の適切な機能テストにリンクさせることができる。
テストを実施しないパラメータ／特性については、開発者はそのパラメータ／特性に関する TOE のコンポーネントの性能が適切に維持されるようガイダンスを作成し、利用者に提供する。
Therefore, in the evaluation activity for the QKD protocol implementation:
従って、QKD プロトコル実装の評価アクティビティでは：

(1) In ASE class:
The evaluator checks that the QKD protocol linked to the correct security proof already verified is assigned to the SFR (see Subsection 8.2).
ASE クラスで
評価者は、既に検証された正しいセキュリティ証明にリンクされた QKD プロトコルが SFR に割り付けられている事をチェックする（8.2 節参照)。

(2) In ADV class:
ADV クラスで、

a) The evaluator examines that the behaviour of the QKD protocol described in the security proof is completely and accurately instantiated in the functional specification and the TOE design (see Subsections 3.1 and Subsection 8.3).
評価者は、セキュリティ証明に記述された QKD プロトコルのふるまいが、機能仕様や TOE 設計の中で、完全、且つ、正確に具体化されている事を検査する（3.1 節及び 8.3 節参照)。

b) The evaluator examines that the assumptions of the security proof are completely and accurately described in terms of the testable parameters/characteristics in the functional specification or the TOE design (see Subsections 3.1 and Subsection 8.3).
評価者は、セキュリティ証明の仮定が、テスト可能なパラメータ／特性の観点から、完全、且つ、正確に機能仕様または TOE 設計へ記述されている事を検査する（3.1 節及び 8.3 節参照)。

(3) In AGD class:
AGD クラスで、
The evaluator examines that the operational user guidance to provides a routine inspection measure to ensure the performance of TOE components related to parameters/characteristics that are not tested (see Subsection 3.2 and Subsection 8.4).
評価者は、利用者操作ガイダンスが、テストを実施しないパラメータ/特性に関連する TOE コンポーネントの性能を保証するための定期点検手段を提供していることを確認する（3.2 節と 8.4 節参照)。

(4) In ATE class:
ATE クラスで、

a) The developer tests functional tests described in Section 10 as developer's tests (see also Subsection 3.3).
開発者は、開発者テストとして 10 章の機能テストを実施する(3.3 節も参照)。

b) The evaluator examines that the developer's tests demonstrate the behaviour of the QKD protocol implementation described in the functional specification and the TOE design (see Subsection 3.3, Subsection 8.5 and Section 10).
評価者は、開発者のテストが、機能仕様や TOE 設計に記述された QKD プロトコル実装のふるまいを実証していることを検査する(3.3 節、8.5 節と 10 章参照)。

c) The evaluator examines that the developer's tests demonstrate the testable parameters/characteristics

described in the functional specification and the TOE design (see Subsection 3.3, Subsection 8.5 and Section 10).

評価者は、開発者のテストが、機能仕様または TOE 設計に記述されたテスト可能なパラメータ／特性を実証していることを検査する(3.3 節、8.5 節と 10 章参照)。

(5) In AVA class:

AVA クラスで、

a) The evaluator assesses vulnerabilities caused by the deviations between the assumptions in the security proof and the corresponding testable parameters/characteristics, and identifies possible potential vulnerabilities in the TOE. It is not necessary to determine how this affects the security parameters (see Subsection 8.6).

AVA クラスで、評価者は、セキュリティ証明の仮定と、それに対応するテスト可能なパラメータ／特性のずれに起因する脆弱性を分析し、TOE で可能性がある潜在的脆弱性を識別する。これがセキュリティパラメータにどのように影響するかを決定する必要はない（8.6 節参照)。

b) The evaluator conducts penetration testing for the identified potential vulnerabilities.

評価者は、識別された潜在的脆弱性について侵入テストを実施する。

1.4.3. Approval of security proof

This document assumes that the developer or the sponsor has submitted the security proof associated with the QKD protocol to a responsible organization prior to evaluation process. Evaluation of the security proofs themselves is not part of the evaluation for QKD protocol implementation. The security proof shall be approved by the responsible organization. The responsible organization may take the opinion of experts, such as a standards developing organization, into account for approval of the security proof. The developer or the sponsor shall provide the evaluation body with the complete, correct, and comprehensible security proof and a detailed correspondence of the assumptions in the security proof to the implementation as evaluation evidence.

この文書は、開発者またはスポンサーが、評価プロセスの前に、QKD プロトコルに関連付けられたセキュリティ証明を責任のある組織に提出したことを前提としている。セキュリティ証明自体の評価は、QKD プロトコル実装評価の一部ではない。セキュリティ証明は、責任のある組織によって承認されなければならない。責任のある組織は、セキュリティ証明を承認するために、標準開発組織などの信頼できるグループの意見を考慮に入れることがある。開発者または申請者は、完全で、正確で、理解しやすいセキュリティ証明と、セキュリティ証明の仮定と実装の詳細な対応を、評価証拠として評価機関へ提供しなければならない。

2. Evaluation method dependencies

This document does not depend on any other evaluation method.
この文書は他の評価方法に依存しない。

3. Required inputs

The required inputs from the developer are shown in the SARs refinements below.
開発者からの必要な入力は、以下の SAR の詳細化に示されている。

3.1. ADV: Development

3.1.1. ADV_FSP.2.1C, ADV_FSP.4.1C

ADV_FSP.2.1C	*The functional specification shall completely represent the TSF.*
ADV_FSP.4.1C	*The functional specification shall completely represent the TSF.* *機能仕様は完全に TSF を表現しなければならない。*
Refinement:	**The functional specification shall completely identify the assumptions in the security proof. The identification of assumptions should be consistent with the identification of the assumption families in Table 3-1 and their detailed descriptions in Section 9 of this document.**
詳細化：	**機能仕様はセキュリティ証明における仮定を完全に識別しなければならない。仮定の識別は、本文書の Table 3-1 の仮定ファミリおよびそれらの詳細な記述（9 章）の識別と整合しているべきである。**

The refinements of ADV_FSP.2.1C and ADV_FSP.4.1C aim at providing the knowledge for conducting vulnerability analysis and testing upon the TOE, as described in the AVA and ATE classes, and require that the assumptions in the security proof are completely identified in the functional specification.
ADV_FSP.2.1C 及び ADV_FSP.4.1C の詳細化では、AVA クラス及び ATE クラスで記述されている TOE に対する脆弱性分析とテストを実施するための知識を与えることを目的としており、セキュリティ証明における仮定が機能仕様において完全に識別されていることを要求している。

3.1.2. ADV_FSP.2.3C, ADV_FSP.4.3C

ADV_FSP.2.3C	*The functional specification shall identify and describe all parameters associated with each TSFI.*
ADV_FSP.4.3C	*The functional specification shall identify and describe all parameters associated with each TSFI.* *機能仕様は、各 TSFI に関連するすべてのパラメータを識別及び記述しなければならない。*
Refinement:	**The functional specification shall identify and describe the testable parameters/characteristics, which can be mapped to each of all the identified assumptions in the security proof.**
詳細化：	**機能仕様書は、セキュリティ証明において識別されたすべての仮定に対応付けられる、テスト可能なパラメータ／特性を識別し、記述しなければならない。**

The refinements of ADV_FSP.2.3C and ADV_FSP.4.3C require the identification and the description of feasible, concrete, and preferably quantitative testing methods for the assumptions in the security proof. Therefore, testable

physical parameters or characteristics shall be mapped to the assumptions in the security proof. For example, if the security proof assumes that "the phase of the pulses are completely random", a good concrete description would be "the phase of the pulses are indistinguishable from a random state using specified statistical methods". The description of the testable parameters/characteristics should reflect either design target values or estimated values based on existing knowledge of them.

In this document, the assumptions commonly used in relevant security proofs of the QKD protocol are addressed and their concrete definitions are provided in Section 9. Their assumption names and the corresponding testable parameters/characteristics are shown in Table 3-1. This mapping is provisional and may contain some differences between the meanings of the assumptions and the corresponding testable parameters/characteristics. However, identifying the corresponding testable parameters/characteristics in ADV activity and demonstrating them in ATE activity is useful for AVA activity.

ADV_FSP.2.3C 及び ADV_FSP.4.3C の詳細化では、セキュリティ証明の仮定について、実行可能で、具体的で、できれば定量的なテスト方法を特定し、記述することが要求される。したがって、テスト可能な物理的パラメータ又は特性を、セキュリティ証明の仮定に対応付けなければならない。例えば、セキュリティ証明が「パルスの位相が完全にランダムである」と仮定している場合、具体的な記述としては、「パルスの位相は、指定された統計的手法を用いるとランダムな状態と区別できない」とするのが良いだろう。テスト可能なパラメータ／特性の記述は、設計目標値か、それらに関する既存の知識に基づく推定値のいずれかを反映すべきである。

本書では、QKD プロトコルのセキュリティ証明で一般的に使用される仮定を取り上げ、9 章でその具体的な定義を示す。それらの仮定の名前と対応するテスト可能なパラメータ／特性を Table 3-1 に示す。このマッピングは暫定的なものであり、仮定の意味と対応するテスト可能なパラメータ／特性との間に若干の相違が含まれる可能性がある。しかし、ADV アクティビティにおいて対応するテスト可能なパラメータ/特性を特定し、ATE アクティビティにおいてそれを実証することは、AVA アクティビティにおいて有用である。

Based on the mapping, each assumption in the security proof can be identified as either of two types:

(i) the assumption is described quantitatively and verifiable by functional tests,

(ii) otherwise.

If type (i) is the case, no vulnerability analysis is required. Otherwise, an assessment of vulnerabilities against the attacks identified for the assumption is necessary.

If the security proof requires a privacy amplification ratio based on the assumptions of realistic characteristics, the developer shall describe the testable parameters/characteristics corresponding to the implemented privacy amplification ratio.

このマッピングに基づき、セキュリティ証明における各仮定は 2 つのタイプのいずれかに分類される：

(i) 仮定が定量的に記述され、機能テストによって検証可能であること。

(ii) その他。

セキュリティ証明が、現実的な特性の仮定に基づく秘匿性増強率を必要とする場合、開発者は、実装された秘匿性増強率に対応するテスト可能なパラメータ／特性を記述しなければならない。

Table 3-1: Assumption families commonly used in security proofs and testable parameters/characteristics mapped to each family.

Classification	Assumption family and testable parameters/characteristics mapped to it
QKD transmitter	**Phase randomization** This family involves assumptions of the phase distribution of the light source, which is ideally indistinguishable from a uniform random distribution. Detailed description is given in Subsubsection 9.1.1. The assumptions can be tested by observing interference between the light pulses. This measurement tests the phase characteristic of output from the light pulse source, rather than phase characteristic of output from the QKD transmitter. In other words, the phase characteristic before attenuating is measured. (Optional) If the phase characteristic is expressed using statistical characteristics, the statistical method should be identified. Functional tests are described in Subsubsection 10.3.2.1 (also refer to ISO/IEC23837(2) 7.7). The related penetration test is described in Subsubsection 11.1.1. このファミリには、光源の位相分布の仮定であり、それは理想的に一様なランダム分布と区別がつかない。詳細な説明は 9.1.1 節を参照。この仮定は、光パルス間の干渉を観察することで検証できる。この測定では送信機からの出力の位相特性ではなく、パルス源からの出力の位相特性をテストする。つまり、減光前の位相特性を測定する。(オプション) 位相特性を、統計特性を使用して表現する場合、その統計手法を特定すべきである。 機能テストは 10.3.2.1 に記述されている（ISO/IEC23837(2) 7.7 も参照のこと）。 関係する侵入テストは 11.1.1 項に記述されている。
	Photon statistics and intensity This family involves assumptions of the photon number statistics, ideally such that the photon number in each encoded pulse emitted from the QKD transmitter follows a Poisson distribution with a given mean photon number μ. Detailed description is given in Subsubsection 9.1.2. For decoy method, the test is sufficient to measure the ratio of probabilities p(1)/p(2) for signal pulses and decoy pulses, where p(n) is the probability that a pulse contains n photons. Functional tests are described in Subsubsection 10.3.2.2 (also refer to ISO/IEC23837(2) 7.2). このファミリは光子数統計の仮定を含み、理想的には、QKD 送信機から送信される各符号化パルス内の光子数が、所定の平均光子数 μ のポアソン分布に従うことを意味する。詳細な説明は 9.1.2 節を参照。デコイ法では、信号パルスとデコイパルスの確率 p(1)/p(2)の比を測定するテストで十分である。ここで、p(n)は、パルスが n 個の光子を含む確率である。 機能テストは 10.3.2.2 に記述されている（ISO/IEC23837(2) 7.2 も参照のこと）。
	Degrees of freedom This family involves assumptions of the degrees of freedom of light used by the QKD transmitter to encode the information, ideally such that the characteristics of the intentionally unused degrees of freedom for encoding are independent of the encoded photon state. Detailed description is given in Subsubsection 9.1.3. These assumptions can be tested by measuring the characteristics of each encoded photon state of degrees of freedom other than those used to encode the information. For example, if the polarization of photon pulses is used to encode, the measurement includes the spectrum (wavelength), time waveform, and phase of the photon pulses. Functional tests are described in Subsubsection 10.3.2.3 (also refer to ISO/IEC23837(2) 7.6). The related penetration test is described in Subsubsection 11.1.2 (tentative). このファミリは、QKD 送信機が情報を符号化する際に使用する光の自由度の仮定を含む。理想的には、符号化のために意図的に使用されない自由度の特性が、符号化された光子状態とは独立していることが望ましい。詳細については、9.1.3 項を参照。この仮定は、情報を符号化する際に使用する自由度以外の自由度の特性を測定することで検証され

Classification	Assumption family and testable parameters/characteristics mapped to it
	る。例えば、光子パルスの偏光が符号化に使用される場合、測定には光子パルスのスペクトラム（波長）、時間波形、位相が含まれる。 機能テストは 10.3.2.3 に記述されている（ISO/IEC23837(2) 7.6 も参照のこと）。 関係する侵入テストは 11.1.2 項（暫定）に記述されている。
	Security and cryptographic boundaries This family involves assumptions of the cryptographic boundaries of the QKD transmitter, ideally such that no reading of the internal settings of the QKD transmitter unit can be conducted from the outside, nor any modification of its internal components. Detailed description is given in Subsubsection 9.1.4. These assumptions correspond to the assumptions of the PP concerning physical protected environment. If the transmitter implements a countermeasure against optical injection attacks, its functionality must be verified. Functional tests are described in Subsubsection 10.3.2.4 (also refer to ISO/IEC23837(2) 7.8, 7.9, and 7.10). The related penetration test is described in Subsubsection 11.1.3. このファミリは、QKD 送信機の暗号境界に関する仮定が含まれ、理想的には、QKD 送信ユニットの内部設定の読み取りは外部からは不可能であり、また内部コンポーネントの変更も不可能である。詳細は 9.1.4 項を参照。この仮定は、物理的に保護された環境に関する PP の前提条件に対応される。送信機が光注入攻撃に対する対策を実装している場合、その機能性を検証する必要がある。 機能テストは 10.3.2.4 に記述されている（ISO/IEC23837(2) 7.8, 7.9, 7.10 も参照すること）。 関係する侵入テストは 11.1.3 項に記述されている。
	Accuracy of the encoding This family involves assumptions of the accuracy of the encoding, ideally such that the QKD transmitter modulates a characteristic of the photon state to the expected value. Detailed description is given in Subsubsection 9.1.5. This assumption is tested in terms of fidelity or distance between the ideal photon states and those under examination. Functional tests are described in Subsubsection 10.3.2.5 (also refer to ISO/IEC23837(2) 7.5). The related penetration test can be performed by the method described in Subsubsection 11.1.4. このファミリは、符号化の正確性に関する仮定が含まれ、理想的には送信機が光子状態の特性を期待値に変調する。詳細については、9.1.5 項を参照のこと。この仮定は理想的な光子状態と検査中の光子状態との間の忠実度または距離という観点から検証される。 機能テストは 10.3.2.5 に記述されている（ISO/IEC23837(2) 7.5 も参照すること）。 関係する侵入テストは 11.1.4 項に記述されている方法に従って行うことができる。
	Independence of adjacent pulses This family involves assumptions of the correlation between adjacent pulses, ideally such that the intensity of emitted pulses is independent of the intensity modulation pattern. Detailed description is given in Subsubsection 9.1.6. These assumptions can be tested by measuring correlation of the pulse intensities to the adjacent pulse states. Functional tests are described in Subsubsection 10.3.2.6 (also refer to ISO/IEC23837(2) 7.4). このファミリは、隣接するパルスの相関の仮定を含み、理想的には放出パルスの強度が強度変調パターンに依存しない。詳細は 9.1.6 項を参照。この仮定は、隣接するパルス状態に対するパルス強度の相関を測定することで検証される。 機能テストは Subsubsection 10.3.2.6 に記述されている（ISO/IEC23837(2) 7.4 も参照のこと）。

Classification	Assumption family and testable parameters/characteristics mapped to it
QKD receiver	**Detection efficiency** This family involves assumptions of the detection efficiency of the detectors, ideally such that it is independent of each basis or bit value. Detailed description is given in Subsubsection 9.2.1. These assumptions are tested by measuring the detection efficiencies of the photon detectors. If mechanisms are implemented to counteract differences in the detection efficiency, a function test should be performed to confirm the validity of the mechanisms (reference to specification of the mechanisms). Functional tests are described in Subsubsection 10.3.3.1 (also refer to ISO/IEC23837(2) 8.2). このファミリは、検出器の検出効率の仮定を含み、理想的には検出器の検出効率が各基底またはビット値に依存しない。詳細は 9.2.1 項を参照のこと。この仮定は、光子検出器の検出効率を測定することで検証される。検出効率の差異を相殺するメカニズムが実装されている場合、そのメカニズムの妥当性を確認するために機能テストを行うべきである（メカニズムの仕様を参照）。機能テストは 10.3.3.1 に述べられている（ISO/IEC23837(2) 8.2 も参照のこと）。
	Degrees of freedom This family involves assumptions of the degrees of freedom of the detection unit used by the QKD receiver, ideally such that the detection unit reacts always in the same way irrespective of the degree of freedom into which the quantum signal is encoded. Detailed description is given in Subsubsection 9.2.2. These assumptions can be tested by measuring the detection efficiency of the photon detectors. In this measurement, photon characteristics are varied in the designed range for all the degrees of freedom of a photon. Functional tests are described in Subsubsection 10.3.3.2 (also refer to ISO/IEC23837(2) 8.2). The related penetration tests on {time, wavelength, polarization}-shift attacks are described in Subsubsection 11.2.1, which can be waived, if the receiver passes the function test described in Subsubsection 10.9.2.2. このファミリは、QKD 受信機で使用される検出ユニットの自由度の仮定を含み、理想的には量子信号が符号化される自由度の度合いに関わらず、検出ユニットが常に同じ方法で反応する。詳細な説明は、9.2.2 項を参照。この仮定は、光子検出器の検出効率を測定することで検証される。この測定では、光子の特性が、光子のすべての自由度に対して設計された範囲内で変化する。 {時間、波長、偏光}-シフト攻撃に関する関連する侵入テストについては、11.2.1 項で説明されている。ただし、10.9.2.2 項で説明されている機能テストに受信機が合格している場合は、これらのテストは必須ではない。 機能テストは 10.3.3.2 に記述されている（ISO/IEC23837(2) 8.2 も参照のこと）。
	Security boundary on optical channel This family involves assumptions that no reading of the internal settings of the QKD receiver unit can be conducted from the outside, nor any modification of its internal components. Detailed description is given in Subsubsection 9.2.3. These assumptions correspond to the assumptions of the PP concerning physically protected environment. If the receiver implements a countermeasure against attacks, such as Trojan horse attack and back-flash attack, its functionality must be verified. Functional tests are described in Subsubsection 10.3.3.3 (also refer to ISO/IEC23837(2) 8.3, 8.4 and 8.5). The related penetration tests described in Subsubsection 11.2.2 can be waived, if the receiver passes the function test. このファミリは、QKD 受信ユニットの内部設定を外部から読み取ったり、内部コンポーネントを変更したりすることはできないという仮定を含む。詳細は 9.2.3 項を参照のこと。 この仮定は、物理的に保護された環境に関する PP の前提条件に対応する。

Classification	Assumption family and testable parameters/characteristics mapped to it
	受信機がトロイの木馬攻撃やバックフラッシュ攻撃などの攻撃に対する対策を実装している場合、その機能性を検証しなければならない。 機能テストは 10.3.3.3 に記述されている（ISO/IEC23837(2) 8.3、8.4 および 8.5 も参照すること）。 受信機が機能試験に合格した場合、11.2.2 項に記載されている関連する侵入テストは必須ではない。
	Accuracy of the demodulation This family involves assumptions that an ideal receiver can perfectly distinguish the two optical modes used for encoding on the chosen basis. Detailed description is given in Subsubsection 9.2.4. The functional test is described in Subsubsection 10.3.3.4. The penetration test for the attack is described in Subsubsection 11.2.4. このファミリは、理想的な受信機は、選択した基底の符号化に用いられる2つの光学モードを完全に弁別できるという仮定を含む。詳細は 9.2.4 項を参照のこと。 機能テストは 10.3.3.4.項に記述されている。 この攻撃に対する侵入テストは 11.2.4 項に記述されている。
	Single-photon sensitivity This family involves assumptions of the detection efficiency in the context of bright illumination attacks, ideally such that the single photon sensitivity of the QKD receiver is not controlled by injected bright light. Detailed description is given in Subsubsection 9.2.5. These assumptions can be tested by measuring the detection efficiency of the photon detector under the illumination of bright light. A set of the functional tests are given in Subsubsection 10.3.3.5 and 10.9.1.1 to evaluate the resistance against the bright illumination attack (also refer to ISO/IEC23837(2) 8.6). The penetration test for the attack is described in Subsubsection 11.2.3. このファミリは、QKD 受信機の単一光子感度が注入された明光によって制御されないという仮定を含む。詳細は 9.2.5 項を参照。この仮定は、明光の照射下における単一光子検出器の検出効率を測定することで検証される。明光攻撃に対する耐性を評価するために、一連の機能試験は 10.3.3.5 および 10.9.2.1 に記載されている（ISO/IEC23837(2) 8.6 も参照すること）。 侵入テストは 11.2.3 項に記述されている。
	Recovery or dead time This family involves assumptions of the dead time of the photon detector, ideally such that the photon detector in the QKD receiver always detects a single photon. In other words, the raw data excludes the detection events during the dead time of any photon detectors. Detailed description is given in Subsubsection 9.2.6. The test is similar to that for single-photon sensitivity, but attack should be done during the dead-time of the photon detectors. The tests should consider properly dead-time width, detection window width of the photon detectors, and gate pulse width for gate-mode detectors (if any). The functional tests are described in Subsubsection10.3.3.6. (also refer to ISO/IEC23837(2) 8.7). The penetration test for the attack is described in Subsubsection 11.2.5 このファミリは、明光攻撃の文脈における検出効率の仮定を含み、理想的には QKD 受信機の単一光子検出器が常に単一光子を検出する。言い換えれば、生データは、単一光子検出器のデッドタイム中の検出イベントを除外する。詳細は、9.2.6 項を参照。 このテストは単一光子感度に対するテストと類似しているが、攻撃は単一光子検出器のデッドタイム中に行う必要がある。この試験では、デッドタイム幅、単一光子検出器の検出ウィンドウ幅、ゲートモード検出器（該当する場合）のゲートパ

Classification	Assumption family and testable parameters/characteristics mapped to it
	ルス幅を適切に考慮する必要がある。機能テストは 10.3.3.6 に記述されている（ISO/IEC23837(2) 8.7 も参照すること）。 侵入テストは 11.2.5 項に記述されている。
Whole of the TOE	**Calibration** This family involves assumptions of calibration, ideally such that the optical signals exchanged in the Calibration phase and the data exchanged in the Post-Processing phase cannot be exploited by attacker to enhance her attack against the QKD system. Detailed description is given in Subsubsection 9.3.1. Functional tests are described in Subsubsection 10.3.4.1 (also refer to ISO/IEC23837(2) 9.1 and 9.2). The related penetration tests described in Subsubsection 11.3.1 can be waived, if the receiver passes the function test. This assumption corresponds to the specification of the calibration. The developer should refer the specification in the functional specification or the TOE design. このファミリは、キャリブレーションの仮定を含み、理想的には、キャリブレーションフェーズで交換される光信号と、後処理フェーズで交換されるデータは、攻撃者が QKD システムに対する攻撃を強化するために利用することはできないことを意味する。詳細は 9.3.1 項を参照。 機能テストは 10.3.4.1 に記述されている（ISO/IEC23837(2) 9.1 および 9.2 も参照のこと）。 受信機が機能テストに合格した場合、11.3.1 項で説明されている関連の侵入テストは免除される。 この仮定は、キャリブレーションの仕様に対応する。開発者は、機能仕様または TOE 設計の仕様を参照するべきである。
	Stability of the light source and the photon detector This family involves assumptions of the stabilities, ideally such that the QKD transmitter and the QKD receiver are typically assumed to remain stable, and the characteristics are the same as when they were characterised. Detailed description is given in Subsubsection 9.3.2. Functional tests are described in Subsubsection 10.3.4.2 (also refer to ISO/IEC23837(2) 7.3). This family corresponds to the stability of the light source in QKD transmitter and the photon detectors in QKD receiver. The developer should refer the user guidance statement which is required by the refinement of AGD_OPE.1.5C in Subsubsection 3.2.2. このファミリは、安定性の仮定を含み、理想的には QKD セッション中、送信機と受信機は通常、安定した状態を維持し、特性評価時と同等であることを意味する。詳細は、9.3.2 項を参照。機能テストは 10.3.4.2 に記述されている（ISO/IEC23837(2) 7.3 も参照のこと）。 このファミリは、QKD 送信機の光子源と QKD 受信機の単一光子検出器の安定性に対応する。開発者は、3.2.2 項の AGD_OPE.1.5C の詳細化によって要求される利用者ガイダンスステートメントを参照するべきである。
	Robustness against provoked damage This family involves assumptions of robustness, ideally such that the light source in the QKD transmitter and the photon detectors in the QKD receiver works properly. Detailed description is given in Subsubsection 9.3.3. Functional tests are described in Subsubsection 10.3.4.3 (also refer to ISO/IEC23837(2) 8.9). This assumption corresponds to robustness of the light source of the QKD transmitter and the photon detectors in the QKD receiver. But no countermeasures are currently known to completely prevent damage to the light source or the photon detector. The developer should refer the user guidance statement which is required by the refinement of AGD_OPE.1.5C in Subsubsection 3.2.2.

Classification	Assumption family and testable parameters/characteristics mapped to it
	このファミリは堅牢性の仮定を含み、理想的には QKD 送信機の光子源と QKD 受信機の単一光子検出器が適切に動作していることを意味する。詳細は、9.3.3 項を参照。 機能テストは 10.3.4.3 に記述されている（ISO/IEC23837(2) 8.9 も参照のこと）。 この仮定は、送信機の光子源と受信機の単一光子検出器の堅牢性に対応する。しかし、光子源と単一光子検出器の損傷を完全に防ぐための対抗策は現時点では知られていない。開発者は、3.2.2 項の AGD_OPE.1.5C の詳細化によって要求される利用者ガイダンスステートメントを参照するべきである。
	Authenticated classical channel This family involves assumptions of the authenticated classical channel, ideally such that the authenticated classical channel provides assured identification of the end point from which channel data was sent and protection of the channel data from modification. Functional tests described in Subsection 10.2. このファミリは認証済み古典チャネルの仮定を含み、理想的には認証済み古典チャネルはチャネルデータが送信されたエンドポイントの保証された識別、及び改変からのチャネルデータの保護を提供することである。 機能テストは 10.2 節に記述されている。
	Random number generator This family involves assumptions of the random number generator, ideally such that the random number generator provides random bits that meets the defined quality metric. Functional tests described in Subsection 10.6. このファミリは乱数生成器の仮定を含み、理想的には乱数生成器が定義された品質の乱数を提供することを含む。 機能テストは 10.6 節に記述されている。

3.1.3.ADV_ARC.1.2C

ADV_ARC.1.2C	*The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.* *セキュリティアーキテクチャ記述は、**TSF** によって維持されるセキュリティドメインを、**SFR** と一貫する形で記述しなければならない。*

Refinement: **The developer shall describe how to isolate the environment used by untrusted users.**

詳細化： **開発者は、信頼できない利用者が使用する環境を、どの様にして分離するかを記述しなければならない**

Security domains refer to environments supplied by the TSF to separate domains for use by potentially-harmful entities; for example, a typical secure operating system supplies a set of resources (address space, per-process environment variables) for use by processes with limited access rights and security properties. Such domains depend on the SFR described in the ST. For example, in the ST which is compliant to [PP-EAL4], the Administrator and Maintainer are trusted due to assumption A,Maint. But Key Requester and Auditor may not be trusted. If the processes run by such untrusted users exist, it may be harmful. So the environments used by such process shall be security domains.

セキュリティドメインとは、TSF によって提供される、有害な可能性があるエンティティが使用するドメインから分離するための環境を指す。例えば、一般的なセキュアなオペレーティングシステムでは、アクセス権やセキュリティ特性が制限されたプロセスにより使用される一連の資源(アドレス空間、プロセスごとの環境変数など)

が提供される。このようなドメインは、ST で記述されている SFR に依存する。例えば、[PP-EAL4]準拠の ST では、前提条件 A.Maint により、管理者と保守担当者は信頼できる。ただし、鍵リクエスタと監査人は信頼できない可能性がある。もし、これらの信頼できない利用者が実行するプロセスが存在するならば、それは有害である可能性がある。従って、このようなプロセスで使用される環境はセキュリティドメインである。

On the other hand, in the ST which is compliant to [PP-EAL2], the operator and all IT products are trusted due to A.OPERATOR and A.IT_PRODUCTS. Since any actions on behalf of users are not allowed before the user is authenticated, no processes run by untrusted users exist if the developer implements SFRs completely and accurately. Therefore, security domains are not necessary.

一方、[PP-EAL2]準拠の ST では、A.OPERATOR と A.IT_PRODUCTS により、オペレーターと全ての IT 製品は信頼できる。利用者が認証されるまで利用者に代わって実行されるアクションは許可されていないため、開発者が SFR を完全かつ正確に実装しているならば、信頼できない利用者が実行するプロセスは存在しない。つまり、セキュリティドメインは必要ない。

3.1.4.ADV_ARC.1.4C

ADV_ARC.1.4C	*The security architecture description shall demonstrate that the TSF protects itself from tampering.* *セキュリティアーキテクチャ記述は、TSF が改ざんから自分自身を保護することを実証しなければならない。*

Refinement: **Active probing attacks via the QKD link are considered as attacks that tamper behaviour of the TSF. The security architecture that resists such attacks is one of TSF's self-protection mechanisms. The security architecture description shall contain how the TSF resists active probing attacks and achieves self-protection.**

詳細化： **QKD リンクを介したアクティブプロービング攻撃は、TSF の動作を改ざんする攻撃と見なされる。このような攻撃に抵抗するセキュリティアーキテクチャは、TSF の自己保護メカニズムの 1 つである。セキュリティアーキテクチャ記述は、TSF がどの様にしてアクティブプロービング攻撃に抵抗し、自己保護を達成するかも含まなければならない。**

The self-protection mechanism shown in the refinement is related to FPT_PHP.3 in the PP. Even if the specifications for implementing FTP_PHP.3 are shown in the functional specification and the TOE design, the developer shall comprehensively describe which specification resists what type of the attack and how resists the attack in the security architecture description.

詳細化に示されている自己保護メカニズムは、PP の FPT_PHP.3 に関連する。FTP_PHP.3 を実装するための仕様が、機能仕様と TOE 設計に示されている場合でも、開発者は、セキュリティアーキテクチャ記述で、どの仕様がどのタイプの攻撃に抵抗し、どの様に攻撃に抵抗するかを包括的に記述しなければならない。

3.1.5.ADV_ARC.1.5C

ADV_ARC.1.5C	*The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.* *セキュリティアーキテクチャ記述は、TSF が SFR 実施機能性のバイパスを防ぐことを実証しなければならない。*

Refinement: **Side channel attacks over the QKD link are considered as bypass of the SFR-enforcing**

functionality. The security architecture that prevents such side channel is one of TSF's bypass prevention mechanisms. The security architecture description shall contain how the TSF prevents side channel attacks.

詳細化： QKD リンク上のサイドチャネル攻撃は、SFR 実施機能のバイパスと見なされる。このようなサイドチャネルを防止するセキュリティアーキテクチャは、TSF のバイパス防止メカニズムの 1 つである。セキュリティアーキテクチャ記述は、TSF がどの様にサイドチャネル攻撃を防ぐかも含まなければならない。

The bypass prevention mechanism shown in the refinement is related to FPT_EMS.1 in the PP. Even if the specifications for implementing FPT_EMS.1 are shown in the functional specification and the TOE design, the developer should comprehensively describe which specification prevents what type of the attack and how counters the attack in the security architecture description.

詳細化に示されているバイパス防止メカニズムは、PP の FPT_EMS.1 に関連している。 FPT_EMS.1 を実装するための仕様が、機能仕様と TOE 設計に示されている場合でも、開発者は、セキュリティアーキテクチャ記述で、どの仕様がどのタイプの攻撃を防止し、どのように攻撃に対抗するかを包括的に記述するべきである。

3.2. AGD: Guidance documents

3.2.1. AGD_OPE.1.3C

AGD_OPE.1.3C	*The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.* *利用者操作ガイダンスは、利用可能な機能とインターフェース、特に利用者の管理下にあるすべてのセキュリティパラメータを、必要に応じてセキュアな値を示し、利用者の役割ごとに記述しなければならない。*

Refinements: The operational user guidance shall provide a procedure for each user role to limit the value of the key establishment attempt counter to secure range. If applicable, the guidance shall contain secure value of the attempt counter threshold. And any security implications related to the management of attempt counter limit shall be detailed.

詳細化： 利用者操作ガイダンスは、試行カウンタの値をセキュアな範囲に制限するための各利用者役割の手順を提供しなければならない。該当する場合、ガイダンスは、試行カウンタしきい値のセキュアな値を含まなければならない。また、試行カウンタ制限管理に関連するセキュリティへの影響についても詳しく説明されなければならない。

3.2.2. AGD_OPE.1.5C

AGD_OPE.1.5C	*The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.* *利用者操作ガイダンスは、TOE の操作のすべての可能なモード(障害や操作誤りの後の操作を含む)、それらの結果、及びセキュアな運用を維持するために必要なことを識別しなければならない。*
Refinements:	The operational user guidance shall provide the TOE user with routine inspection measures to ensure that there is no performance degradation due to aging in and no damage to the light source in the QKD transmitter and the photon detector in the QKD receiver. The guidance shall contain necessary user actions to maintain secure operation if any performance degradation or damage is identified in either component.
詳細化：	利用者操作ガイダンスは、QKD 送信機の光源と QKD 受信機の単一光子検出器に経年変化による性能劣化がないこと、損傷がないことを確認するための定期的な検査手段を、TOE 利用者に提供しなければならない。ガイダンスは、いずれか部品の性能劣化または損傷が検出された場合に、セキュアな運用を維持するために必要な利用者アクションも含んでいなければならない。

3.3. ATE: Tests

3.3.1. ATE_COV.1.1C

ATE_COV.1.1C	*The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.* *テストカバレージの証拠は、テスト証拠資料におけるテストと機能仕様における TSFI との間の対応を提示しなければならない。*
Refinements:	The evidence of the test coverage shall contain the correspondence between the tests in the test documentation and the testable parameters/characteristics mapped to the assumptions in the security proof in the functional specification.
詳細化：	テストカバレッジの証拠は、テスト証拠資料におけるテストと、機能仕様におけるセキュリティ証明の仮定にマッピングしたテスト可能なパラメータ／特性との間の対応を含まなければならない。

See Table 3-1 for the mapping between the assumptions in the security proof and the testable parameters/characteristics.
セキュリティ証明の仮定とテスト可能なパラメータ／特性とのマッピングについては、Table 3-1 参照のこと。

3.3.2. ATE_COV2.2C

ATE_COV.2.2C	*The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.* *テストカバレージの分析は、機能仕様におけるすべての TSFI がテストされていることを実証しなければならない。*
Refinements:	The analysis of the test coverage shall contain the correspondence between the tests in the

test documentation and the testable parameters/characteristics mapped to the assumptions in security proof in the functional specification.

詳細化： テストカバレッジの分析は、テスト証拠資料におけるテストと、機能仕様におけるセキュリティ証明の仮定にマッピングしたテスト可能なパラメータ／特性との間の対応を含まなければなければならない。

See Table 3-1for the mapping between the assumptions in the security proof and the testable parameters/characteristics.

セキュリティ証明の仮定とテスト可能なパラメータ／特性とのマッピングについては、Table 3-1 を参照のこと。

3.3.3.ATE_FUN.1.1C

ATE_FUN.1.2C	*The test documentation shall consist of test plans, expected test results and actual test results.* *テスト証拠資料は、テスト計画、期待されるテスト結果、及び実際のテスト結果から構成されなければならない。*

Refinements: The test plan shall include functional tests described in Section 10.

テスト計画は 10 章の機能テストを含まなければならない。

4. Required tool types

The functional tests and the penetration tests identified in this document require some optical tools. The tools are listed in Table 12-1. The developer and the evaluator may choose the required tools for each functional test or the penetration test.
この文書で識別されている機能テストと侵入テストには、いくつかの光学機器が必要になる。機器は Table 12-1 にリストされている。開発者と評価者は、機能テストまたは侵入テストごとに必要な機器を選択してよい。

5. Required evaluator competences

The evaluator for the QKD modules shall be able to link the penetration tests shown in Section 11 to the implementation of the TOE and shall be able to judge the validity of the results of the penetration tests. The following knowledge is required.

QKD 評価者は、TOE の実装に対して、この SD に示される侵入テストを結びつけることができ、また侵入テストの結果の妥当性を判断できなければならない。次のような知識が必要である。

1. Basic knowledge of the QKD Protocol
   量子鍵配送プロトコルの基本的な知識
2. Knowledge of CC to understand PP and SD
   PP 及び SD を理解するための CC の知識
3. Knowledge of QKD module
   QKD モジュールの知識
   A. to understand vendor QKD protocol implementation and QKD module security architecture
      ベンダーの QKD プロトコル実装と QKD モジュールセキュリティアーキテクチャを理解するため
   B. to select appropriate penetration tests that can test vulnerabilities of the TOE, understanding vendor's QKD protocol implementation and QKD module security architecture and to build the penetration test step by step
      ベンダーの QKD プロトコルの実装と QKD モジュールセキュリティアーキテクチャの理解から、TOE の脆弱性をテストできる侵入テストを選択し、ステップバイステップで侵入テストを構築できる

6. Requirements for reporting

The evaluation activities in this document start from SARs and are defined in conjunction with CEM work units. Therefore, the evaluator may include the report of the evaluation activity in the report of the CEM work unit.
この文書の評価アクティビティは SAR から始まり、CEM ワークユニットと組み合わせて定義されている。従って、評価者は、CEM ワークユニットの報告に本評価アクティビティの報告を含めてよい。

7. Rationale for the evaluation method

A rationale is given at the level of the evaluation method below to show that the derivation of the evaluation activities in an evaluation method, from the original work units in the CEM, is appropriate.
評価方法における評価アクティビティが、CEM の元のワークユニットから適切に導出されたことを示す根拠を評価方法のレベルで示す。
This may be given either at the level of the evaluation method, or at the level of individual evaluation activities.
これは、評価方法のレベル、又は個々の評価アクティビティのレベルのいずれかで与えることができる。

The following rationale shows that the evaluation activities in this evaluation method are appropriately derived from the original work units of the CEM at the level of the evaluation method.
次に示す根拠が、この評価方法における評価アクティビティが、CEM の元のワークユニットから適切に導出されたことを、評価方法のレベルで示す。

The evaluation method shall include a rationale that the derivation of the evaluation activities from work units in the CEM.
評価方法は CEM のワークユニットから評価アクティビティを導出するための根拠を含まなければならない。

That rationale may contain an explanation of why work units were modified for the scope and depth of an evaluation of a specific technology or TOE type.
その根拠は、特定の技術又は TOE 種別の評価の範囲及び深さのために、なぜワークユニットが作り直されたかの説明を含めることができる。

The TOE to which this SD applies is QKD modules that implements Decoy-state BB84 with time-bin encoding, one of the QKD protocols. The deviations between the assumptions in the security proof and the actual TOE characteristics corresponding to the assumptions may compromise the security of the QKD protocol and should be treated as potential vulnerabilities in the QKD modules. Since there is no original work unit that handles such deviations, the evaluation activity was derived.
この SD が適用される TOE は、QKD プロトコルの一つである Decoy-state BB84 with time-bin encoding を実装した QKD モジュールである。QKD プロトコルでは、セキュリティ証明における仮定と、仮定に対応する実際の TOE の特性との間のずれが QKD プロトコルのセキュリティを危険にさらす可能性があり、QKD モジュールにおいてこのずれを潜在的脆弱性として扱うべきである。このようなずれを扱う元のワークユニットは存在しないため、評価アクティビティを導出した。

The rationale shall further state how the evaluation activities it contains address all aspects of the action elements in CC Part 3 to which they apply.
その根拠は、さらに、その評価アクティビティが、適用される CC パート 3 のアクションエレメントの全ての側面にどのように対処するかを述べなければならない。

The developer action elements use the elements already defined in CC Part 3 without modification.
開発者アクションエレメントは、CC Part 3 に定義済みのエレメントをそのまま使用する。
The content and presentation elements are defined in Section 3 by detailing the information required for the evaluation activity.

内容・掲示エレメントは、評価アクティビティに必要な情報を詳細化して 3 章に定義している。
The evaluator action elements use the elements already defined in CC Part 3 without modification.
評価者アクションエレメントは CC Part 3 に定義済みのエレメントをそのまま使用する。

It shall also justify that the manner in which the action elements or work units are addressed is complete with respect to the evaluation context in which the evaluation method is intended to be applied.
評価方法の適用が意図されている評価コンテキストに関して、アクションエレメント又はワークユニットに対処する方法が完全であることを正当化しなければならない。

The unique context of the evaluation for the QKD protocol implementation involves assessing the deviations between assumptions in security proofs and the actual implementation characteristics of the TOE, as well as evaluating the vulnerabilities arising from these deviations.
Section 1 addresses these aspects by mapping the testable parameters/characteristics to the assumptions and integrating them into functional tests, ensuring a robust evaluation framework tailored to QKD protocol implementation. The evaluation framework is structured using assurance classes: ASE, ADV, ATE, AGD and AVA. Each class provides specific procedures for evaluating the QKD protocol, including identification of a security proof, examining functional specifications, conducting functional tests, maintaining performance through the operational user guidance and assessing potential vulnerabilities.
In Section 3, the content and presentation elements are detailed, and the necessary evaluation evidence is identified.
In Section 8, the following evaluation activities are also defined:

- identification of security proofs and QKD protocols in the ASE class,
- instantiation in specifications and design documents in the ADV class,
- demonstration through testing in the ATE class,
- maintaining performance through the operational user guidance in AGD class, and
- vulnerability analysis in the AVA class.

The developer action element and evaluator action element remain unchanged.
By maintaining these elements, it ensures that evaluators can effectively obtain the necessary evaluation evidence, assess the deviations between security proofs and implementation, and thoroughly evaluate the behaviour of the QKD protocol, thereby ensuring that all elements and work units are completely addressed.
QKD プロトコルの実装に対する評価の一意なコンテキストは、セキュリティ証明における仮定と TOE の実際の実装特性との間のずれを評価すること、およびこれらのずれから生じる脆弱性を評価することである。
1 章では、テスト可能なパラメータ/特性を仮定にマッピングし、それを機能テストに統合することによって、この側面に対処し、QKD プロトコルの実装に合わせた堅牢な評価フレームワークを保証する。評価の枠組みは、ASE、ADV、ATE、AGD、AVA という保証クラスを使用して構成される。各クラスは、セキュリティ証明の確認、機能仕様の検査、機能テストの実施、利用者操作ガイダンスによる性能維持、潜在的な脆弱性の評価など、QKD プロトコルの評価に特化した手順を提供する。
3 章では、内容と掲示エレメントについて詳述し、必要な評価エビデンスを特定する。
8 章では、以下の評価アクティビティも定義する：

- ASE クラスにおけるセキュリティ証明と QKD プロトコルの識別、
- ADV クラスにおける仕様書及び設計書への具体化、
- ATE クラスにおけるテストによる実証、
- AGD クラスにおける利用者操作ガイダンスによる性能維持、および
- AVA クラスにおける脆弱性分析。

開発者アクションエレメントと評価者アクションエレメントに変更はない。
これらのエレメントを維持することで、評価者が必要な評価証拠を効果的に入手し、セキュリティ証明と実装の間のずれを評価し、QKD プロトコルの動作を徹底的に評価することができ、それによってすべてのエレメントとワークユニットが完全に対処されていることを保証する。

8. Evaluation activities

8.1. Objective

Evaluation Activities (EA) aims to support evaluation for the SFRs of QKD protocols associated with security proofs in the ADV class, evaluation of developer tests in the ATE class and analysing vulnerabilities in the AVA class. The evaluator performs the work units as presented in the CEM. In addition, the evaluator ensures evaluation evidence satisfies EAs specified in the following subsections.

EA は、セキュリティ証明を伴った QKD プロトコルの SFR の ADV クラスの評価、ATE クラスの開発者テストの評価、AVA クラスの脆弱性分析をサポートすることを目的としている。評価者は CEM に示されているようにワークユニットを実行する。さらに、評価者は、評価証拠が以下の節で指定されている EA を満たしていることを保証する。

8.2. ASE: Security Target Evaluation

8.2.1. ASE_REQ.2-11

ASE_REQ.2-11	*The evaluator shall examine the statement of security requirements to determine that all assignment operations are performed correctly.* *評価者は、すべての割付操作が正しく実行されることを決定するために、セキュリティ要件のステートメントを検査しなければならない。*
Evaluation Activity:	**For assignment of QKD protocol, the evaluator shall check the protocol is associated with to security proofs approved by a responsible organization.**
評価アクティビティ	**QKD プロトコルの割付けに関して：評価者は、プロトコルに責任のある機関によって承認されたセキュリティ証明が伴っていることをチェックしなければならない。**

This evaluation activity is related to the assignment for the extended SFR FCS_QKD.1.1 defined in [PP-EAL4] or [PP-EAL2].

この評価アクティビティは、[PP-EAL4]または[PP-EAL2]で定義された拡張 SFR FCS_QKD.1.1 の割付けに関連している。

8.3. ADV: Development

8.3.1. ADV_ARC.1-2

ADV_ARC.1-2	*The evaluator shall examine the security architecture description to determine that it describes the security domains maintained by the TSF.* *評価者は、TSF によって維持されるセキュリティドメインをセキュリティアーキテクチャが記述していることを決定するために、その記述を検査しなければならない。*
Evaluation Activity:	**The evaluator shall examine the security architecture description to determine how the TSF isolates the environment used by untrusted users.**
評価アクティビティ	**評価者は、TSF が、信頼できない利用者が使用する環境を、どの様に分離するかを決定する為に、セキュリティアーキテクチャ記述を検査しなければならない。**

8.3.2.ADV_ARC.1-4

ADV_ARC.1-4	*The evaluator shall examine the security architecture description to determine that it contains information sufficient to support a determination that the TSF is able to protect itself from tampering by untrusted active entities.* *評価者は、セキュリティアーキテクチャ記述が、信頼できない能動的なエンティティによる改ざんから TSF が自分自身を保護できるという決定を支持するのに十分な情報を含んでいることを決定するために、その記述を検査しなければならない。*
Evaluation Activity:	The evaluator shall examine the security architecture description to determine how the TSF resists active probing attacks and achieves self-protection.
評価アクティビティ	評価者は、TSF が、アクティブプロービング攻撃にどの様に抵抗し、自己保護を達成するかを決定する為に、セキュリティアーキテクチャ記述を検査しなければならない。

8.3.3.ADV_ARC.1-5

ADV_ARC.1-5	*The evaluator shall examine the security architecture description to determine that it presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.* *評価者は、SFR 実施メカニズムをバイパスできないようにするしくみを適切に説明する分析をセキュリティアーキテクチャ記述が提示していることを決定するために、その記述を検査しなければならない。*
Evaluation Activity:	The evaluator shall examine the security architecture description to determine how the TSF prevents side channel attacks.
評価アクティビティ	評価者は、TSF が、サイドチャネル攻撃をどの様に防ぐかを決定する為に、セキュリティアーキテクチャ記述を検査しなければならない。

8.3.4.ADV_FSP.2-1, ADV_FSP.4-1

ADV_FSP.2-1	*The evaluator shall examine the functional specification to determine that the TSF is fully represented.*
ADV_FSP.4-1	*The evaluator shall examine the functional specification to determine that the TSF is fully represented.* *評価者は、TSF が完全に表現されていることを決定するために、機能仕様を検査しなければならない。*
Evaluation Activity:	The evaluator shall examine the functional specification to determine that it completely identifies all assumptions in the security proof.
評価アクティビティ	評価者は、機能仕様が、セキュリティ証明の仮定を識別していることを決定するために、機能仕様を検査しなければならない。

8.3.5.ADV_FSP.2-4, ADV_FSP.4-5

ADV_FSP.2-4	*The evaluator shall examine the presentation of the TSFI to determine that it completely identifies all parameters associated with every TSFI.* *評価者は、TSFI の提示がすべてのTSFI に関連するすべてのパラメータを完全に識別していることを決定するために、その提示を検査しなければならない。*
ADV_FSP.4-5	*The evaluator shall examine the presentation of the TSFI to determine that it completely identifies all parameters associated with every TSFI.* *評価者は、TSFI の提示がすべてのTSFI に関連するすべてのパラメータを完全に識別していることを決定するために、その提示を検査しなければならない。*
Evaluation Activity:	The evaluator shall examine the functional specification to determine that it completely identifies all the testable parameters/characteristics mapped to the assumptions in the security proof.
評価アクティビティ	評価者は、機能仕様が、セキュリティ証明の仮定にマップされるすべてのテスト可能なパラメータ／特性を識別していることを決定するために、機能仕様を検査しなければならない。

See Table 3-1 for the correspondence between the assumptions and the testable parameters/characteristics.
仮定とテスト可能なパラメータ／特性の対応については、Table 3-1 を参照のこと。

8.3.6. ADV_FSP.2-5, ADV_FSP.4-6

ADV_FSP.2-5	*The evaluator shall examine the presentation of the TSFI to determine that it completely and accurately describes all parameters associated with every TSFI.* *評価者は、TSFI の提示がすべてのTSFI に関連するすべてのパラメータを完全かつ正確に記述していることを決定するために、その提示を検査しなければならない。*
ADV_FSP.4-6	*The evaluator shall examine the presentation of the TSFI to determine that it completely and accurately describes all parameters associated with every TSFI.* *評価者は、TSFI の提示がすべてのTSFI に関連するすべてのパラメータを完全かつ正確に記述していることを決定するために、その提示を検査しなければならない。*
Evaluation Activity:	The evaluator shall examine the functional specification to determine that it completely and accurately describes all the testable parameters/characteristics mapped to the assumptions in the security proof.
評価アクティビティ	評価者は、機能仕様が、セキュリティ証明の仮定にマップされたすべてのテスト可能なパラメータ／特性を完全かつ正確に記述していること決定するために、機能仕様を検査しなければならない。

The security proof document contains the security proof and defines the assumptions of the security proof. Generally, the functional specification document which is created during developing the TOE and the security proof document are issued separately. For this reason, the developer needs to describe the assumptions in the security proof in the functional specification document without omission or excess.
セキュリティ証明文書には、セキュリティ証明が記述されており、セキュリティ証明の仮定が定義されている。一般的に、TOE 開発時に作成される機能仕様書とセキュリティ証明文書は、それぞれ個別に発行される。そのため、開発者は、セキュリティ証明の仮定を機能仕様書に過不足なく記述する必要がある。

The accuracy of the descriptions of the testable parameters/characteristics does not mean that the values of the ideal/realistic characteristics in the assumption of the security proof and the corresponding values of the testable parameters/characteristics in the functional specification match exactly.
In some cases, the assumption is described with the values of the ideal characteristics, but the corresponding values in the functional specification are design target values or estimated values based on existing knowledge of the testable parameters/characteristics. In this case, it is considered accurate if the functional specification describes the values of the testable parameters/characteristics in Table 3-1.
テスト可能なパラメータ／特性の記述の正確さは、セキュリティ証明の仮定における理想的／現実的な特性の値と、機能仕様におけるテスト可能なパラメータ／特性の対応する値が完全に一致することを意味しない。
場合によっては、仮定は理想的な特性の値で記述されるが、機能仕様における対応する値は、設計目標値またはテスト可能なパラメータ／特性に関する既存の知識に基づく推定値である。この場合、機能仕様に Table 3-1 のテスト可能なパラメータ／特性の値が記述されていれば、正確であるとみなされる。
On the other hand, the assumption is described with the values of realistic characteristics (especially when determining the privacy amplification ratio), the corresponding values in the functional specification shall be consistent. For example, in the case of phase randomization, if the privacy amplification ratio is determined by assuming that the deviation between the realistic phase and the ideal randomized phase is 10, the deviation between the realistic phase and the ideal random phase shall be described also in the functional specification, and the value shall be within 10.
一方、現実的な特性値（特に秘匿性増強率を決定する場合）を仮定に記述する場合は、機能仕様の対応する値を整合させなければならない。例えば、位相ランダム化の場合、現実的な位相と理想的なランダムな位相とのずれを 10 と仮定して秘匿性増強率を決定する場合、現実的な位相と理想的なランダムな位相とのずれを機能仕様書にも記述し、その値は 10 以内でなければならない。

8.3.7.ADV_FSP.2-9, ADV_FSP.4-11

ADV_FSP.2-9	*The evaluator shall examine the functional specification to determine that it is a complete instantiation of the SFRs.* *評価者は、機能仕様が SFR の完全な具体化であることを決定するために、その仕様を検査しなければならない。*
ADV_FSP.4-11	*The evaluator shall examine the functional specification to determine that it is a complete instantiation of the SFRs.* *評価者は、機能仕様が SFR の完全な具体化であることを決定するために、その仕様を検査しなければならない。*
Evaluation Activity:	**The evaluator shall examine the functional specification to determine that it is a complete instantiation of external behaviour of the QKD protocol described in the security proof.**
評価アクティビティ	**評価者は、機能仕様がセキュリティ証明に記述された QKD プロトコルの外部のふるまいの完全な具体化であることを決定するために、その仕様を検査しなければならない。**

8.3.8.ADV_FSP.2-10, ADV_FSP.4-12

ADV_FSP.2-10	*The evaluator shall examine the functional specification to determine that it is an accurate instantiation of the SFRs.* *評価者は、機能仕様が SFR の正確な具体化であることを決定するために、その仕様を検査しなければならない。*
ADV_FSP.4-12	*The evaluator shall examine the functional specification to determine that it is an accurate instantiation of the SFRs.* *評価者は、機能仕様が SFR の正確な具体化であることを決定するために、その仕様を検査しなければならない。*
Evaluation Activity:	The evaluator shall examine the functional specification to determine that it is an accurate instantiation of external behaviour of the QKD protocol described in the security proof.
評価アクティビティ	評価者は、機能仕様がセキュリティ証明に記述された QKD プロトコルの外部のふるまいの正確な具体化であることを決定するために、その仕様を検査しなければならない。

8.3.9.ADV_TDS.1-7, ADV_TDS.3-15

ADV_TDS.1-7	*The evaluator shall examine the TOE security functional requirements and the TOE design, to determine that all ST security functional requirements are covered by the TOE design.* *評価者は、すべての ST セキュリティ機能要件が TOE 設計に含まれることを決定するために、TOE セキュリティ機能要件及びTOE 設計を検査しなければならない。*
ADV_TDS.3-15	*The evaluator shall examine the TOE security functional requirements and the TOE design, to determine that all ST security functional requirements are covered by the TOE design.* *評価者は、すべての ST セキュリティ機能要件が TOE 設計に含まれることを決定するために、TOE セキュリティ機能要件及びTOE 設計を検査しなければならない。*
Evaluation Activity:	The evaluator shall examine the security proof and the TOE design, to determine that all behaviour(s) of the QKD protocol described in the security proof are covered by the TOE design.
評価アクティビティ	評価者は、セキュリティ証明に記述されたすべての QKD プロトコルのふるまいが TOE 設計に含まれることを決定するために、セキュリティ証明及び TOE 設計を検査しなければならない。

8.3.10.ADV_TDS.1-8, ADV_TDS.3-16

ADV_TDS.1-8	*The evaluator shall examine the TOE design to determine that it is an accurate instantiation of all security functional requirements.* *評価者は、TOE 設計がすべてのセキュリティ機能要件の正確な具体化であることを決定するために、そのTOE 設計を検査しなければならない。*
ADV_TDS.3-16	*The evaluator shall examine the TOE design to determine that it is an accurate instantiation of all security functional requirements.* *評価者は、TOE 設計がすべてのセキュリティ機能要件の正確な具体化であることを決定するために、そのTOE 設計を検査しなければならない。*
Evaluation Activity:	The evaluator shall examine the TOE design to determine that it is an accurate instantiation of all behaviour of the QKD protocol described in the security proof.

評価アクティビティ　評価者は、TOE 設計がセキュリティ証明に記述された QKD プロトコルのすべてのふるまいの正確な具体化であることを決定するために、その TOE 設計を検査しなければならない。

8.4. AGD: Guidance documents

8.4.1. AGD_OPE.1-3

AGD_OPE.1-3	*The evaluator shall examine the operational user guidance to determine that it describes, for each user role, the available security functionality and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.* *評価者は、利用者操作ガイダンスが、利用可能なセキュリティ機能性とインターフェース、特に利用者の管理下にあるすべてのセキュリティパラメータを、適切にセキュアな値を示して、利用者の役割ごとに記述していることを決定するために、そのガイダンスを検査しなければならない。*

Evaluation Activity: The evaluator shall examine the operational user guidance to determine that it describes for each user role, a procedure to limit the value of the key establishment attempt counter to secure range. If the TSF provides management function of the attempt counter threshold, the evaluator shall examine that the description contains secure value of the attempt counter threshold.

評価アクティビティ　評価者は、利用者操作ガイダンスが、試行カウンタの値をセキュアな範囲に制限する手順を、利用者役割ごとに記述していることを決定するために、そのガイダンスを検査しなければならない。TSF が試行カウンタしきい値の管理機能を提供する場合、評価者は、その記述に試行カウンタしきい値のセキュアな値が含まれていることを検査しなければならない。

Evaluation Activity: The evaluator shall examine the operational user guidance to determine that it details security implications related to the management of the attempt counter limit.

評価アクティビティ　評価者は、利用者操作ガイダンスが、試行カウンタ制限管理に関連するセキュリティへの影響を詳しく説明していることを決定するために、そのガイダンスを検査しなければならない。

8.4.2. AGD_OPE.1-5

AGD_OPE.1-5	*The evaluator shall examine the operational user guidance and other evaluation evidence to determine that the guidance identifies all possible modes of operation of the TOE (including, if applicable, operation following failure or operational error), their consequences and implications for maintaining secure operation.* *評価者は、利用者操作ガイダンスがTOE の操作のすべての可能なモード(必要に応じて、障害または操作誤りの後の操作を含む)、それらの結果及びセキュアな運用を維持するために必要なことを識別していることを決定するために、そのガイダンスとその他の評価証拠を検査しなければならない。*

Evaluation Activity: The evaluator shall examine that the operational user guidance provides the TOE user with routine inspection measures to ensure that there is no performance degradation due to

aging in and no damage to the light source in the QKD transmitter and the photon detector in the QKD receiver.

評価アクティビティ　評価者は、利用者操作ガイダンスが、送信機の光源と受信機の光子検出器に経年変化による性能劣化がないこと、損傷がないことを確認するための定期的な検査手段を、TOE 利用者に提供していることを検査しなければならない。

Evaluation Activity: The evaluator shall examine that the operational user guidance contains necessary user action to maintain secure operation if any performance degradation or damage is identified in either component.

評価アクティビティ　評価者は、いずれかの部品の性能劣化または損傷が検出されたときに、セキュアな運用を維持するために必要な利用者アクションが、利用者操作ガイダンスに含まれていることを検査しなければならない。

8.5. ATE: Tests

8.5.1. ATE_COV.1-1

ATE_COV.1-1	*The evaluator shall examine the test coverage evidence to determine that the correspondence between the tests identified in the test documentation and the TSFIs described in the functional specification is accurate.* *評価者は、テスト証拠資料に識別されているテストと機能仕様に記述されている TSFI の間の対応が正確であることを決定するために、テストカバレージ証拠を検査しなければならない。*

Evaluation Activity: The evaluator shall examine the test coverage evidence to determine that the correspondence between the tests identified in the test documentation and the actual characteristics corresponding to the assumptions in the security proof described in the functional specification is accurate.

評価アクティビティ　評価者は、テスト証拠資料に識別されているテストと、機能仕様に記述されているセキュリティ証明の前提に対応する特性との対応が正確であること決定するために、テストカバレージ証拠を検査しなければならない。

Evaluation Activity: The evaluator shall examine the test documentation to determine that functional tests described in Section 10 are performed by the developer.

評価アクティビティ　評価者は、10 章に記述されている機能テストが開発者によって実行されていることを決定するために、テスト証拠資料を検査しなければならない。

8.5.2. ATE_COV.2-4

ATE_COV.2-4	*The evaluator shall examine the test coverage analysis to determine that the correspondence between the interfaces in the functional specification and the tests in the test documentation is complete.* *評価者は、機能仕様におけるインターフェースとテスト証拠資料におけるテストの間の対応が完全であることを決定するために、テストカバレージ分析を検査しなければならない。*

Evaluation Activity: The evaluator shall examine the test coverage evidence to determine that the

	correspondence between the tests identified in the test documentation and the testable parameters/characteristics mapped to the assumptions in the security proof described in the functional specification is complete.
評価アクティビティ	評価者は、テスト証拠資料に識別されているテストと、機能仕様に記述されているセキュリティ証明の仮定にマップされたテスト可能なパラメータ／特性との対応が完全であること決定するために、テストカバレージ証拠を検査しなければならない。
Evaluation Activity:	The evaluator shall examine the test documentation to determine that functional tests described in Section 10 are performed by the developer.
評価アクティビティ	評価者は、10 章に記述されている機能テストが開発者によって実行されていることを決定するために、テスト証拠資料を検査しなければならない。

8.5.3. ATE_FUN.1-1

ATE_FUN.1-1	*The evaluator shall check that the test documentation includes test plans, expected test results and actual test results.* *評価者は、テスト証拠資料にテスト計画、期待されるテスト結果、及び実際のテスト結果が含まれていることをチェックしなければならない。*
Evaluation Activity:	The evaluator shall check the test plan includes the functional tests described in Section 10.
評価アクティビティ	評価者は、10 章に示されている機能テストがテスト計画に含まれていることをチェックしなければならない。

8.6. AVA: Vulnerability Assessment

8.6.1. AVA_VAN.2-3, AVA_VAN.5-3

AVA_VAN.2-3	*The evaluator shall examine sources of information publicly available to identify potential vulnerabilities in the TOE.* *評価者は、TOE の潜在的脆弱性を識別するために、公開の場で利用できる情報源を検査しなければならない。*
AVA_VAN.5-3	*The evaluator shall examine sources of information publicly available to identify potential vulnerabilities in the TOE.* *評価者は、TOE の潜在的脆弱性を識別するために、公開の場で利用できる情報源を検査しなければならない。*
Evaluation Activity:	The evaluator shall examine Section 9 in this document to identify potential vulnerabilities in the TOE.
評価アクティビティ	評価者は、TOE の潜在的脆弱性を識別するために、本文書 9 章を検査しなければならない。

9. Identifying potential vulnerabilities in the TOE

The assumptions in security proofs (whether of ideal characteristics or realistic characteristics) are not always fully met, and there are deviations between these assumptions and the corresponding implementation characteristics of the TOE. Such deviations may compromise the security of QKD protocol and should be treated as potential vulnerabilities in the TOE. This section addresses commonly used assumptions in security proofs of many QKD protocols, identifies known attacks (see Section 11 in detail), and provides vulnerability assessments. To conduct vulnerability analysis and testing upon the TOE, the testable parameters/characteristics are mapped to the assumptions as shown in Section 3.

If an assumption is described quantitatively and can be verified through functional tests, no vulnerability analysis is required. This is because these functional tests ensure that appropriate countermeasures are implemented completely and accurately, and by reflecting the corresponding testable parameters in the privacy amplification ratio, it can be proven through a security proof that the identified attacks do not compromise the security of the QKD protocol. Otherwise, an assessment of vulnerabilities against attacks identified for the assumption is necessary, based on the corresponding testable parameters/characteristics.

セキュリティ証明における仮定（理想的な特性か現実的な特性かに関わらず） は、常に完全に満たされるとは限らず、これらの仮定と TOE の対応する実装特性との間にずれが生じる場合がある。このようなずれは QKD プロトコルを危うくする可能性があり、TOE の潜在的な脆弱性として扱われるべきである。本節では、多くの QKD プロトコルのセキュリティ証明で一般的に使用されている仮定を取り上げ、既知の攻撃（詳細は 11 章を参照）を特定し、脆弱性評定を提供する。TOE に対する脆弱性分析およびテストを実施するために、テスト可能なパラメータ/特性は、3 章に示されているように仮定にマッピングされる。

ある仮定が定量的に記述され、機能テストによって検証できる場合、脆弱性分析は不要である。これは、これらの機能テストにより、適切な対策が完全に正確に実施されることが保証され、対応するテスト可能なパラメータを秘匿性増強率に反映させることで、特定された攻撃によって QKD プロトコルの安全性が危殆化しないことをセキュリティ証明によって証明できるためである。それ以外の場合は、仮定に対して特定された攻撃に対する脆弱性の評価を、対応するテスト可能なパラメータや特性に基づいて行うことが必要となる。

9.1. QKD transmitter

9.1.1. Phase randomization

Description of assumption family:

It is assumed that a pulse (or a pulse pair) emitted by an ideal QKD transmitter is phase-randomized. As a result, the quantum state of encoded pulses is invariant under optical phase shifts. In the case of polarization encoding, the quantum state of an emitted optical pulse is invariant under any amount of polarization-independent optical phase shift. In the case of time-bin encoding (i.e. phase encoding) on a pulse pair, the quantum state of an emitted pulse pair is invariant under any amount of common optical phase shift applied to both pulses. A security proof involves assessment of how much the attacker may learn about the information encoded on an optical pulse (e.g., bit, basis and nominal intensity of decoy-state) by measuring the pulse. If the security proof adopts the above ideal assumption, it amounts to assume that the attacker can gain no more information from attack strategies sensitive to the common optical phase.

理想的な送信機によって放出されたパルス(またはペアのパルス)の位相はランダム化されていると仮定されている。結果として、符号化パルスの量子状態は、光位相シフトによって変化しない。偏光符号化の場合、偏光無

依存の光学位相シフトを出射パルスに印加しても、その量子状態は変化しない。パルス対のタイムビン符号化（つまり、位相符号化）する場合、両パルスに同じ光学位相シフトを与えても、パルス対の量子状態は変化しない。セキュリティ証明では、光パルスに符号化されている情報（ビット値、基底、デコイ状態の名目強度など）を、パルスの測定によって攻撃者がどのくらい取得できるかを評価する。セキュリティ証明がこの仮定を採用する場合、攻撃者が一般的な光位相に敏感な攻撃戦略を採用しても攻撃者が取得できる情報量は増加しないと想定されている。

Description of the attack method:

Source attacks with phase information: An attacker prepares a light source that emits pulses whose optical phases are correlated to those of the pulses emitted from the QKD transmitter. They send the target pulse from the QKD transmitter and another pulse from their light source to an interferometer to acquire a measurement outcome. If the QKD transmitter does not satisfy the ideal assumption, the outcome may depend on the optical phase difference between the two pulses. The attacker can then estimate the information encoded on the target pulse based on the measurement outcome. This knowledge may allow for a higher probability of QKD key estimation. For example, if the phase of the pulse encoding bit "1" is not random and has a unique phase, the attacker can estimate in which pulse bit "1" is encoded.

位相情報を用いた攻撃：攻撃者は、QKD 送信機から送信されるパルスの光位相と相関するパルスを放出する光源を用意する。攻撃者は、QKD 送信機からターゲットパルスを送信し、もう 1 つのパルスを光源から送信し、干渉計に送って測定結果を取得する。もし仮定が満たされていないと、この測定結果は 2 つのパルスの光学位相差に依存する。すると、攻撃者は測定結果に基づいて対象パルスに符号化されていた情報を推定することができる。例えば、ビット”1”を符号化したパルスの位相がランダムでなく、固有の位相を持っていたならば、攻撃者は、ビット”1”がどのパルスに符合されているか推定する事が出来る。

Assessment:

If the security proof specifies relevant quantitative assumptions and those assumptions can be verified by functional testing, no further analysis is required.

If it is not the case, assessment of vulnerabilities against the attack described above is necessary, which is detailed in the following.

もし、セキュリティ証明が、関連する定量的な前提を指定し、その前提が機能テストによって検証できるならば、それ以上の分析は必要ない。

そうでない場合は、上記の攻撃に対する脆弱性の評価が必要であり、その評価は以下に詳細化する。

The known attacks assume that the attacker can prepare a light source that emits pulses whose optical phases are correlated to those of the pulses emitted from the QKD transmitter. If the light source used in the QKD transmitter is a gain-switched laser or other pulsed lasers in which the laser oscillation ceases after emission of each pulse, penetration tests are not necessary because preparation of such a light source is not possible with current technology. There has been no demonstration of injection locking with a single seed pulse that contains only one photon or less on average.

If the light source used in the QKD transmitter is a laser that keeps laser oscillation continually, such as a mode-locked laser or a CW laser followed by light intensity modulation, the source attacks with phase information described above using a phase-correlated light source may be performed with current technology. It is necessary to conduct and pass penetration tests. The penetration test for the attack is described in Subsubsection 11.1.1.

既知の攻撃は、攻撃者が、QKD 送信機から発せられるパルスの光位相と相関するパルスを発する光源を用意できることを前提としている。QKD 送信機で使用される光源が、ゲインスイッチ方式レーザや、各パルスの発光

後にレーザ発振が停止する他のパルスレーザーである場合、このような光源の準備は現在の技術では不可能であるため、侵入テストは必要ない。平均で 1 個以下の光子しか含まない単一のシードパルスによる注入同期のデモンストレーションはまだ行われていない。
QKD 送信機で使用される光源が、モードロックレーザや連続波レーザに光強度変調を施したものなど、レーザ発振を継続的に維持するレーザである場合、現在の技術でも、位相相関光源を使用して、上述の位相情報を用いた攻撃を行うことができる。侵入テストを実施してパスする必要がある。攻撃に対する侵入テストは、11.1.1 項で説明されている。

References:

H. -K. Lo and J. Preskill, “Phase randomization improves the security of quantum key distribution”, arXiv:quant-ph/0504209.
H. -K. Lo and J. Preskill, “Security of quantum key distribution using weak coherent states with nonrandom phases”, Quant. Inf. Comput. **8** 431-458 (2007).
Y. -L. Tang *et al*., “S Source attack of decoy-state quantum key distribution using phase information”, Phys. Rev. A **88**, 022308 (2013).

9.1.2. Photon statistics and intensity

Description of assumption family:

It is assumed that the photon number contained in each of the encoded pulse emitted from an ideal QKD transmitter follows a Poisson distribution with a given mean photon number μ. This is an assumption on infinite number of parameters $p(n)$, which are probabilities of the pulse containing $n = 0,1, \dots, \infty$ photons. Some security proofs adopt relaxed assumptions. Some assume that the mean photon number μ is unknown but satisfies $\mu_0 \leq \mu \leq \mu_1$, where μ_0 and μ_1 are known lower and upper bounds. Others directly assume a set of inequalities fulfilled by $p(n)$ instead of requiring an exact Poisson distribution.
理想的な QKD 送信機から送信される符号化パルスに含まれる光子数は、与えられた平均光子数μのポアソン分布に従うと仮定する。これは、$n = 0,1, \dots, \infty$個の光子を含むパルスの確率であるパラメータ$p(n)$が無限にあるという仮定である。一部のセキュリティ証明では、緩やかな仮定を採用している。平均光子数μは不明であるが、$\mu_0 \leq \mu \leq \mu_1$（$\mu_0$と$\mu_1$は既知の下限および上限）を満たすという仮定もある。また、厳密なポアソン分布を要求するのではなく、$p(n)$が満たす不等式の集合を直接仮定するものもある。

Description of the attack method:

Photon-number-splitting (PNS) attack: Although the BB84 protocol was originally designed to encode information on a single photon, most of the current QKD transmitters use lasers which may emit multiple photons at the same time. The attacker can exploit such an occasion to extract one photon and store it in a quantum memory, while they let the remaining photons be received by the QKD receiver possibly with a better efficiency than the transmissivity of the actual quantum channel to enhance the effectiveness of the attack. Since the quantum state of the photons received by the receiver is not disturbed, this attack causes no increase in the bit error rates. After the basis used for each pulse is announced, the attacker can measure the stored photon to know the bit value encoded in the photon.
光子数分割（PNS）攻撃：BB84 プロトコルは、もともと単一光子に情報を符号化するように設計されているが、現在の QKD 送信機のほとんどは、同時に複数の光子を放出する可能性があるレーザを使用している。攻撃者はこのような機会を悪用して 1 つの光子を取り出し、量子メモリに保存することができる。一方で、残りの光子は

実際の量子チャネルの伝送効率よりも高い可能性で QKD 受信機に受信させ、攻撃の有効性を高めることができる。受信機が受信した光子の量子状態は乱されていないため、この攻撃によってビットエラー率が増加することはない。各パルスに使用された基底が発表された後、攻撃者は、光子に符号化されたビット値を知るために、保存された光子を測定することができる。

The decoy-state BB84 protocol counters this type of attacks by monitoring the detection rates for emitted pulses with different intensities. Since the amount of the trace that should be inevitably left by the PNS attack is estimated under the assumptions of Poisson distribution for the emitted photon number, unexpected deviation from Poisson distribution opens a risk of making the PNS attack effective.
Decoy-state BB84 プロトコルは、異なる強度を持つ放出パルスの検出率を監視することで、この種の攻撃に対抗する。PNS 攻撃によって必然的に残される痕跡の量は、放出光子数のポアソン分布を仮定して推測されるため、ポアソン分布からの予期せぬずれは、PNS 攻撃を効果的なものにするリスクを生じさせる。

Conditional beam-splitting attack: A weaker version of the PNS attacks implemented by linear optical devices (optical switches and beam splitters), photon detectors and feed-forward electronics. This attack cannot implement the heralded extraction and storing of a single photon in the PNS attacks, but the extracted photon must be immediately measured in a basis. Otherwise, the function provided by this attack differs from the ideal PNS attacks only quantitatively depending on the internal losses and efficiency of optical devices and the bandwidths of the detectors, the switches, and the electronics.
条件付きビーム分割攻撃：線形光学素子（光スイッチおよびビームスプリッタ）、単一光子検出器、フィードフォワード電子回路によって実装された PNS 攻撃の弱体化バージョン。この攻撃では、PNS 攻撃で予告されていた単一光子の抽出と保存は実装できないが、抽出された光子は直ちに測定されなければならない。さもなければ、この攻撃によって提供される機能は、光デバイスの内部損失と効率、および検出器、スイッチ、電子機器の帯域幅に依存する量的な差異のみで、理想的な PNS 攻撃とは異なるものとなる。

Assessment:
If the security proof specifies relevant quantitative assumptions and those assumptions can be verified by functional testing, no further analysis is required.
If it is not the case, assessment of vulnerabilities against the attack described above is necessary, which is detailed in the following.
セキュリティ証明に関連する定量的な仮定が指定され、その仮定が機能テストによって検証できる場合、それ以上の分析は必要ない。
そうでない場合は、上記の攻撃に対する脆弱性の評価が必要であり、その評価は以下に詳細化する。
The PNS attack described above is possible in principle, but this is not feasible with current technology. Therefore, penetration test(s) are not necessary.
The conditional beam-splitting attack described above can be performed with current technology. However, there is no known detailed strategy to make it work on the decoy-state BB84 protocol. Therefore, penetration test(s) are not necessary.
上述の PNS 攻撃は原理的には可能だが、現在の技術では実現できない。したがって侵入テストは必要ない。
上述の条件付きビーム分割攻撃は、現在の技術でも実行可能である。しかし、decoy-state BB84 プロトコルで動作させるための詳細な戦略は知られていない。したがって、侵入テストは必要ない。

References:

M. Dušek, et al., “Generalized beam-splitting attack in quantum cryptography with dim coherent states”, Opt. Comm. 169, 103 (1999).

J. Calsamiglia, et al., “Removal of a single photon by adaptive absorption”, Phys. Rev. A 64, 043814 (2001).

J. Calsamiglia, et al., “Conditional beam-splitting attack on quantum key distribution”, Phys. Rev. A 65, 012312 (2001).

9.1.3. Degrees of freedom

Description of assumption family:

It is assumed that pulses from an ideal QKD transmitter leak no information on their encoding to any degrees of freedom of light other than the degree of freedom that the protocol uses for encoding (e.g. polarization or time-bin).

理想的な QKD 送信機からのパルスは、プロトコルが符号化に使用する自由度（例えば、偏光やタイムビン）以外の光の自由度には、符号化に関するいかなる情報も漏らさないと想定されている。

Description of the attack method:

Intercept-resend attack with side information: The attacker intercepts the encoded pulse(s) by detecting a photon that is in a specific mode of the proper degree of freedom and matches to a mode description in other degrees of freedom at the same time. When detection succeeds, the attacker resends another photon in the same mode of the proper degree of freedom. For example, in the case of time-bin encoding when the pulses from the transmitter nominally have V polarization, the attacker may detect a H-polarized photon in the time-bin mode corresponding to the Z-basis and the bit value 0. When detection succeeds, the attacker resends a V-polarized photon in the time-bin mode corresponding to the Z-basis and the bit value 0. If the pulses from the transmitter have nonnegligible H polarization components only for the Z-basis state, this attack causes no bit errors in the X basis.

サイド情報による Intercept-resend 攻撃：正規の自由度の特定のモードにあり、かつ他の自由度のあるモード条件に合致する光子を検出することで、符号化されたパルスを傍受する。検出に成功すると、攻撃者は正規の自由度における同じモードの別の光子を再送する。例えば、送信機からのパルスが通常 V 偏光であるタイムビン符号化の場合、攻撃者は Z 基底およびビット値 0 に対応するタイムビンモードで H 偏光の光子を検出できる可能性がある。検出に成功した場合、攻撃者は Z 基底およびビット値 0 に対応するタイムビンモードで V 偏光の光子を再送信する。送信機からのパルスが Z 基底状態のみ無視できない H 偏光成分を含む場合、この攻撃によって X 基底ではビットエラーは発生しない。

Side-channel filtering attack: The attacker places in the optical channel a linear optical transmission filter whose transmissivity does not have dependency in the proper degree of freedom but has dependency in other degrees of freedom. For example, in the case of time-bin encoding, the attacker may place a spectral filter. If the two Z-basis states with bit values 0 and 1 have different transmissivity, the bit recorded upon successful detection at the QKD receiver will be biased. If the same filter does not affect the X-basis states, it causes no bit errors in the X basis.

サイドチャネルフィルタリング攻撃：攻撃者は、適切な自由度には依存せず、他の自由度に依存する透過率を持つ線形の光伝送フィルタを光チャネルに配置する。例えば、タイムビン符号化の場合、攻撃者は周波数フィルタを配置する可能性がある。ビット値が 0 と 1 の 2 つの Z 基底状態の透過率が異なる場合、QKD 受信機で正常に検出された際に記録されるビットに偏りが生じる。同じフィルタが X 基底状態に影響を与えない場合、X 基底状態にビットエラーは発生しない。

Quantum nondemolition measurement (QND) attack: There is a quantum process called QND measurement which, when applied to an input photon, produces a measurement outcome and leaves a photon with minimal backaction of the measurement. A variant of this type of measurement may provide a wider variety of input-output relation than the intercept-resend attack, which the attacker may exploit to acquire larger bit information with a smaller increase in the bit error rates.
量子非破壊測定（QND）攻撃：QND 測定と呼ばれる量子プロセスがあり、入力光子に適用すると測定結果が得られ、測定のバックアクションが最小限の光子が残る。このタイプの測定の変形は、攻撃者がビットエラー率の増加を最小限に抑えながらより多くのビット情報を取得するために利用する可能性がある、Intercept-resend 攻撃よりも多様な入出力関係を提供できる可能性がある。

Photon-number-splitting (PNS) attack and Conditional beam-splitting attack: See the description in Subsubsection 9.1.2. The decoy-state BB84 protocol counters these types of attacks by monitoring the detection rates for emitted pulses with different intensities. Any leak of the information related to the intensity of the pulses through other degrees of freedom opens a risk of making these attacks effective.
光子数分割（PNS）攻撃と条件付きビーム分割攻撃：9.1.2 項の説明を参照のこと。decoy-state BB84 プロトコルは、異なる強度で放出されたパルスの検出率をモニタリングすることで、これらのタイプの攻撃に対抗する。他の自由度を通じてパルス強度に関する情報が漏洩すると、これらの攻撃が有効になるリスクが生じる。

Assessment:
If the security proof specifies relevant quantitative assumptions and those assumptions can be verified by functional testing for a degree of freedom, no further analysis is required for the degree of freedom.
If it is not the case, assessment of vulnerabilities against the attack described above is necessary, which is detailed in the following.
The intercept-resend attack with side information described above can be performed with current technology. It is necessary to conduct and pass penetration tests.
The side-channel filtering attack described above can be performed with current technology. It is necessary to conduct and pass penetration tests. The penetration test for the attack is described in Subsubsection 11.1.2.
The QND attack described above is possible in principle, but this is not feasible with current technology. Therefore, penetration test(s) are not necessary.
The PNS attack described above is possible in principle, but this is not feasible with current technology. Therefore, penetration test(s) are not necessary.
The conditional beam-splitting attack described above can be performed with current technology. However, there is no known detailed strategy to make it work on the decoy-state BB84 protocol. Therefore, penetration test(s) are not necessary.

セキュリティ証明に関連する定量的な仮定が指定され、その仮定が自由度の機能テストによって検証できる場合、自由度に対するそれ以上の分析は必要ない。
そうでない場合は、上記の攻撃に対する脆弱性の評価が必要であり、その評価は以下に詳細化する。
上述のサイド情報付き Intercept-resend 攻撃は、現在の技術でも実行可能である。侵入テストを実施し、合格する必要がある。

上述のサイドチャネルフィルタリング攻撃は現在の技術で実行可能である。侵入テストを実施し、合格する必要がある。攻撃に対する侵入テストは、11.1.2 項で説明されている。
上述の QND 攻撃は原理的には可能だが、現在の技術では実行不可能である。したがって、侵入テストは必要ない。
上述の PNS 攻撃は原理的には可能だが、現在の技術では実行不可能である。したがって、侵入テストは必要ない。
上述の条件付きビーム分割攻撃は、現在の技術でも実行可能である。しかし、decoy-state BB84 プロトコルで機能させるための詳細な戦略は知られていない。したがって、侵入テストは必要ない。

9.1.4. Security and cryptographic boundaries

Description of assumption family:

It is assumed that an ideal QKD transmitter allows no reading of its internal settings and no modification of its internal components.
理想的な QKD 送信機の内部設定を読み取ったり、内部コンポーネントを変更したりすることはできないと想定される。

Description of the attack method:

- An attacker reads/writes internal settings of the QKD transmitter.
- An attacker modifies internal components of the QKD transmitter.
- An attacker reads internal confidential data from internal components of the QKD transmitter.
- An attacker observes internal states of the QKD transmitter.

攻撃者は、QKD 送信機の内部設定を読み書きする。
攻撃者は、QKD 送信機の内部コンポーネントを変更する。
攻撃者は、QKD 送信機の内部コンポーネントから、内部の秘密データを読み出す。
攻撃者は、QKD 送信機の内部状態を観察する。
An attacker uses these adverse actions to disclose the QKD key or compromise the QKD transmitter.
攻撃者はこれらの有害なアクションを使用して、QKD 鍵を暴露したり、QKD 送信機を危殆化したりする。
One well-known attack method is the Trojan horse attack. An attacker injects light into the QKD transmitter via the QKD link, observes the reflected light, and estimates the status of modulation optics in the QKD transmitter. From this, the attacker guesses the basis, the bit value, and the intensity choices made by the QKD transmitter.
よく知られている攻撃方法の 1 つは、トロイの木馬攻撃である。攻撃者は、QKD リンクを介して送信機に光を注入し、反射光を観測して QKD 送信機における変調光の状態を推定する。これにより、攻撃者は QKD 送信機が選択した基底とビット値と強度を推測する。

Assessment:

The security and cryptographic boundaries of the QKD transmitter are physically protected due to the assumption of each PP. i.e. A.SecureOp of [PP-EAL4] or A.PHYSICAL of [PP-EAL2]. So an attacker cannot access internal components of the QKD transmitter directly.
The internal settings of the QKD transmitter are protected by user identification and authentication functions and access control functions via user interface(s). So an attacker cannot access internal settings of the QKD transmitter via user interface(s).
If above assumptions are achieved and above functions are implemented completely and accurately, no potential vulnerabilities exist in above point of view.

QKD 送信機のセキュリティ暗号境界は、各 PP の前提条件によって、物理的に保護されている。つまり、[PP-EAL4]の A.SecureOp、または、[PP-EAL2]の A.PHYSICAL である。そのため、攻撃者は QKD 送信機の内部コンポーネントに直接アクセスできない。
QKD 送信機の内部設定は、利用者識別認証機能とアクセス制御機能によって保護されている。そのため、攻撃者は利用者インターフェースを介して QKD 送信機の内部設定にアクセスできない。
上記の前提条件が達成され、上記の機能が完全かつ正確に実装されているならば、上記の観点での潜在的脆弱性は存在しない。
However, the QKD link is not physically protected and not access controlled. An attacker may observe internal state (e.g. choice of encoding basis) of the QKD transmitter via injecting probing light through the QKD link (Trojan horse attack). An attacker may also attempt to modify the characteristics of internal components (e.g. laser source) via irradiation through the QKD link.
しかし、QKD リンクは物理的に保護されておらず、アクセス制御もされていない。攻撃者は、QKD リンクを介して、プローブ光の照射により QKD 送信機の内部状態(例えば、エンコーディング基底の選択)を観察する可能性がある（トロイの木馬攻撃)。また、攻撃者は、QKD リンクを介した光照射により内部コンポーネント（例えばレーザー光源）の特性の変更を試みるかもしれない。

Trojan horse attack countermeasures are implemented in several steps.
1. A light injection monitor is implemented that monitors the light intensity injected into the QKD transmitter.
2. When the light injection monitor detects strong light, the TSF will automatically respond to prevent information leakage due to light reflection. e.g. the TSF performs "emergency stop of the QKD link" (FPT_PHP.3).
3. When light is injected below the detection limit, the maximum reflected light intensity is estimated based on the transmission and reflection characteristics of the QKD transmitter components.

トロイの木馬攻撃の対抗策は、いくつかのステップで実装される。
1. 送信機に注入される光強度を監視する光注入モニタが実装される。
2. 光注入モニタが強い光を検知すると、TSF は自動的に応答し、光の反射による情報漏洩を防ぐ。例えば TSF は、「QKD リンクの緊急停止」を実行する(FPT_PHP.3)。
3. 検出限界以下の光が注入された場合、最大反射光強度は、送信機コンポーネントの透過特性と反射特性に基づいて推定される。

If the security proof specifies quantitative assumptions on the reflected light intensity and those assumptions can be verified by functional testing, no further analysis is required on the Trojan horse attack.
セキュリティ証明が反射光の強度に関する定量的な想定を規定しており、その想定が機能テストで検証できる場合は、トロイの木馬攻撃に関するさらなる分析は必要ない。

If it is not the case, assessment of vulnerabilities against the Trojan horse attack is necessary, which is detailed in the following.
そうでない場合は、上記の攻撃に対する脆弱性の評価が必要であり、その評価は以下に詳細化する。

Among variants of the Trojan horse attacks, one that estimates the choice of pulse intensity must accompany the PNS attack or its variant described in Subsubsection 9.1.2. The PNS attack is possible in principle, but this is not feasible with current technology. The conditional beam-splitting attack can be performed with current technology,

but there is no known detailed strategy to make it work on the decoy-state BB84 protocol. Therefore, penetration tests for this variant of the Trojan horse attack is not necessary.
トロイの木馬攻撃の亜種の中で、パルス強度の選択を推定するものは、9.1.2 節に述べられた PNS 攻撃またはその亜種と組み合わせて用いられる。PNS 攻撃は原理的には可能だが、現在の技術では実現できない。したがって侵入テストは必要ない。条件付きビーム分割攻撃は、現在の技術で実行可能だが、decoy-state BB84 プロトコルで動作させるための詳細な戦略は知られていない。したがって、トロイの木馬攻撃のこの亜種に対する侵入テストは必要ない。

Variants of the Trojan horse attacks that estimate the choice of the basis and the bit value can be performed with current technology. It is necessary to conduct and pass penetration tests. The penetration test for the attack is described in Subsubsection 11.1.3.
トロイの木馬攻撃の亜種で基底とビット値の選択を推定するものは現在の技術で実行可能である。侵入テストを実施し、合格する必要がある。攻撃に対する侵入テストは 11.1.3 項に記述されている。

On the other hand, assessment of the threat of light irradiation altering the characteristics of internal components is given as the following. If a light injection monitor is implemented, strong light injection will be detected. In other words, the intensity of light injection is limited by the detection threshold of the light injection monitor. It has not been reported that the characteristics of linear optical components are affected by light injection with the intensity below the detection threshold. On the other hand, a laser can be affected by injected light due to its nonlinear dynamics. The effect of nonlinearity is most significant when the frequency of the injected light is the same as that of the laser. This situation has been analyzed as the effect of feedback light on a laser. It is reported that the feedback effects are negligible when the light is reinjected into the laser as a fraction smaller than one 10^{-6} of the emitted light. Therefore, the effect of the injected light does not need to be considered if the estimated intensity is less than the above criterion. Otherwise, the TOE should be tested using the test specified in Subsubsection 10.3.2.4.
一方、光照射が内部の素子の特性を変えてしまうという脅威の評価は、以下の通りである。光注入モニタが実装されていると強い注入光は検出される．言い換えれば，注入光の強度は光注入モニタの検出限界で制限される．この検出限界以下の強度の光で線形な光部品が影響を受けることは知られていない．一方、レーザはその非線形ダイナミクスにより、注入光の影響を受けることがある。非線形性の影響が最も大きくなるのは、注入光の周波数がレーザの周波数と同じ場合である。この状況は、レーザに対するフィードバック光の影響として分析されてきた。その結果、レーザに再入射される光が出射光の 100 万分の 1 より小さい場合、フィードバック効果は無視できると報告されている。したがって、注入光の推定強度が上記の基準以下であれば、注入光の影響を考慮する必要はない。そうでない場合は、10.3.2.4 に規定された試験を用いて TOE を試験すること。

Reference

K.Stubkjaer and M. Small, "Noise properties of semiconductor lasers due to optical feedback", *IEEE Journal of Quantum Electronics*, vol. 20, no. 5, pp. 472-478, May 1984, doi: 10.1109/JQE.1984.1072428.

K. I. Kallimani and M. J. O'Mahony, "Relative intensity noise for laser diodes with arbitrary amounts of optical feedback", *IEEE Journal of Quantum Electronics*, vol. 34, no. 8, pp. 1438-1446, Aug. 1998, doi: 10.1109/3.704337.

9.1.5. Accuracy of the encoding

Description of assumption family:

Encoding of the QKD transmitter is performed by modulating the assumed degree of freedom of light. An ideal

QKD transmitter carries out the modulation accurately as implied by the QKD protocol and by the chosen values of protocol parameters. In the case of the decoy-state BB84 protocol, a degree of freedom formed by a pair of optical modes, such as the polarization and the time bin, is used for the encoding of the four states of the BB84 protocol. A set of values for the pulse intensity are specified as protocol parameters of the decoy-state BB84 protocol.
送信機の符号化は、想定される光の自由度を変調することで実行される。理想的な QKD 送信機は、QKD プロトコルおよびプロトコルパラメータの選択された値によって示されるように、正確に変調を実行する。decoy-state BB84 プロトコルの場合は、偏光やタイムビンなどの一対の光モードによって形成される自由度が、BB84 プロトコルの 4 つの状態の符号化に使用される。decoy-state BB84 プロトコルのプロトコルパラメータとして、パルス強度の値のセットが指定されている。

Description of the attack method:
Intercept-resend attack on the monitoring basis: The attacker intercepts the encoded pulse(s) from the QKD transmitter and makes a photon detection to distinguish the two states for the basis used for monitoring, determining a bit value. When the detection was successful, the attacker prepares a stronger optical pulse with the proper modulation corresponding to the determined bit value and sends it to the QKD receiver. This attack introduces no additional errors, but the determined bit value may partially reveal the bit value chosen by the QKD transmitter on the other basis if the encoding is not accurate.
監視用基底への Intercept-resend 攻撃：攻撃者は、QKD 送信機からの符号化パルスを傍受し、監視に使用される基底に対して 2 つの状態を区別する光子検出を行い、ビット値を決定する。検出が成功すると、攻撃者は決定されたビット値に対応する適切な変調を施したより強力な光パルスを準備し、それを QKD 受信機に送信する。この攻撃によって新たなエラーが生じることはないが、符号化が正確でない場合、決定されたビット値によって、もう一方の基底で QKD 送信機が選択したビット値が部分的に明らかになる可能性がある。

Photon-number-splitting (PNS) attack and Conditional beam-splitting attack: See the description in Subsubsection 9.1.2. The decoy-state BB84 protocol counters these types of attacks by monitoring the detection rates for emitted pulses with different intensities. Unexpected deviation of the modulation intensity opens a risk of making these attacks effective.
光子数分割（PNS）攻撃および条件付ビーム分割攻撃：9.1.2 項の説明を参照のこと。decoy-state BB84 プロトコルは、異なる強度の放出パルスの検出率を監視することで、これらの攻撃を防御する。変調強度の予期せぬ偏差は、これらの攻撃を効果的なものにするリスクをもたらす。

Assessment:
If the security proof specifies relevant quantitative assumptions and those assumptions can be verified by functional testing, no further analysis is required.
If it is not the case, assessment of vulnerabilities against the attack described above is necessary, which is detailed in the following.
セキュリティ証明に関連する定量的な仮定が指定され、その仮定が機能テストによって検証できる場合、それ以上の分析は必要ない。
そうでない場合は、上記の攻撃に対する脆弱性の評価が必要であり、その評価は以下に詳細化する。
The PNS attack described above is possible in principle, but this is not feasible with current technology. Therefore, penetration test(s) are not necessary.
上述の QND 攻撃は原理的には可能だが、現在の技術では実行不可能である。したがって、侵入テストは必要な

い。
The conditional beam-splitting attack described above can be performed with current technology. However, there is no known detailed strategy to make it work on the decoy-state BB84 protocol. Therefore, penetration test(s) are not necessary.
上述の条件付きビーム分割攻撃は、現在の技術でも実行可能である。しかし、decoy-state BB84 プロトコルで機能させるための詳細な戦略は知られていない。したがって、侵入テストは必要ない。

The intercept-resend attack on the monitoring basis can be performed with current technology. It is necessary to conduct and pass penetration tests. The penetration test for the attack is described in Subsubsection 11.1.4.
監視用基底への Intercept-resend 攻撃は現在の技術で実行可能である。侵入テストを実施し、合格する必要がある。攻撃に対する侵入テストは、11.1.4 項で説明されている。

9.1.6. Independence of adjacent pulses

Description of assumption family:
The internal states of light source and the modulation components of an ideal QKD transmitter in one communication round are statistically independent of those in the other rounds.
理想的な QKD 送信機のある通信ラウンドにおける光源および変調素子の内部状態は、他のラウンドのそれらと統計的に独立である。

Description of the attack method:
If the internal states such as the choices of bases, bit values, and pulse intensities in one communication round are correlated to the optical pulses emitted in other rounds, the latter pulses serve as a side channel from which the attacker may extract information on the encoding.
もし、ある通信ラウンドにおける基底、ビット値、パルス強度の選択のような内部状態が、他のラウンドで送出された光パルスと相関を持つと、その光パルスはサイドチャネルの役割を果たすことになり、攻撃者が符号化についての情報を引き出す可能性がある。

Assessment:
If the security proof specifies relevant quantitative assumptions and those assumptions can be verified by functional testing, no further analysis is required.
If it is not the case, assessment of vulnerabilities against the attack described above is necessary, which is detailed in the following.
セキュリティ証明に関連する定量的な仮定が指定され、その仮定が機能テストによって検証できる場合、それ以上の分析は必要ない。
そうでない場合は、上記の攻撃に対する脆弱性の評価が必要であり、その評価は以下に詳細化する。
When there are correlations between the internal states of a round and the emitted pulses in other rounds, an attacker may measure the pulses and estimate the status of modulation optics in the QKD transmitter in the former round. From this, the attacker may guess the basis, the bit value, and the intensity choices made by the QKD transmitter. This threat is equivalent to that of the Trojan horse attack on the transmitter described in Subsection 9.2.3 except that the role of the reflection of the injected pulse is substituted by the emitted pulses in the other rounds. This attack can be performed with current technology. It is necessary to conduct and pass penetration tests. The penetration test for the attack can be designed as a modification of the one described in Subsubsection 11.1.3.

あるラウンドの内部状態と、他のラウンドの送出パルスが相関を持つとき、攻撃者はそのパルスを測定することで、前者のラウンドにおける QKD 送信機の変調光学素子の状態を推定するかもしれない。これにより、攻撃者は QKD 送信機が行った基底、ビット値、パルス強度の選択を推測するかもしれない。この脅威は、注入光の反射の役割が他のラウンドの送出パルスに替わったことを除けば、9.2.3 節に記述された送信機に対するトロイの木馬攻撃と同等である。この攻撃は現在の技術で実行可能である。侵入テストを実施し、合格する必要がある。この攻撃に対する侵入テストは、11.1.3 節に記述されているテストを改変することで設計できる。

9.2. QKD receiver

9.2.1. Detection efficiency

Description of assumption family:

It is assumed in most security proofs that the detection efficiency of the detectors is independent of each basis or bit value.

多くのセキュリティ証明では、検出器の検出効率は各基底またはビット値に依存しないと想定される。

Description of the attack method:

An attacker can eavesdrop on the bit value transmitted from the QKD transmitter using man-in-the-middle attack with a certain probability. This certain probability is taken into account in the privacy amplification and the eavesdropped bits are removed from the final QKD key, so this attack method is ineffective.

攻撃者は、中間者攻撃を使用して、送信機から送信されたビット値を一定の確率で盗聴する事ができる。この一定の確率は秘匿性増強で考慮され、盗聴されたビットと最終的な QKD 鍵との相関を取り除くことができるため、この攻撃方法は効果がない。

However, if the detection efficiency differs depending on the basis, an attacker optimizes the eavesdropping strategy for each basis, he may succeed in eavesdropping more than a certain probability.

しかし、基底によって検出効率が異なるならば、攻撃者は基底ごとに盗聴戦略を最適化し、一定確率以上の盗聴を成功させるかも知れない。

Or, for example, if the detection efficiency of bit 0 is lower, the attacker can estimate with high probability that the raw key is bit 1 without even eavesdropping.

または、例えば、ビット 0 の検出効率が低い場合、攻撃者は、盗聴すらせずに高い確率で「生鍵はビット 1 である」と推定できる。

Passive attack based on sifted key inference:

シフト鍵の推論に基づく受動的攻撃：

If the probability for a sifted key bit to have one value, say, 0, is larger than that for the other value, say, 1, distribution of the sifted key is not uniform, and the attacker may exploit that information for guessing the value of the QKD key. This involves no active intervention on the quantum channel and hence leads to no increase in the observed bit error rate.

シフト鍵ビットがある値、例えば 0 を持つ確率が、他の値、例えば 1 を持つ確率よりも大きい場合、シフト鍵の分布は一様ではなく、攻撃者は QKD 鍵の値を推測するためにその情報を利用することができる。そのため、攻撃者はその情報を利用して QKD の鍵の値を推測することができる。この場合、量子チャネルへの能動的な侵入は行われないため、観測されるビット誤り率は増加しない。

Assessment:

If the security proof specifies relevant quantitative assumptions and those assumptions can be verified by functional

testing, no further analysis is required.
If it is not the case, assessment of vulnerabilities against the attack described above is necessary, which is detailed in the following.
もし、セキュリティ証明が、関連する定量的な仮定を指定し、その仮定が機能テストによって検証できるならば、それ以上の分析は必要ない。
そうでない場合は、上記の攻撃に対する脆弱性の評価が必要であり、その評価は以下に詳細化する。

If the two photon detectors for bit values 0 and 1 used for generation of sifted key bits have different detection efficiencies, the probability of a sifted key bit to have one value is larger than that of the other value, leading to potential vulnerability against the passive attack based on sifted key inference described above, can be performed with current technology. The TOE may adopt some mechanisms to cancel out the difference in detection efficiencies, such as inserting an optical attenuator before a detector or randomly changing assignment of the bit values to the two detectors. Since these mitigating mechanisms involve physical means, the cancellation should still be imperfect.
シフト鍵ビットの生成に使用されるビット値 0 と 1 の 2 つの単一光子検出器の検出効率が異なると、シフト鍵ビットが一方の値を持つ確率が他方の値を持つ確率よりも大きくなり、上述のシフト鍵推論に基づく、現在の技術でも実施可能な受動的攻撃に対して潜在的脆弱性となる可能性がある。TOE は、検出器の前に光減衰器を挿入したり、2 つの検出器へのビット値の割り当てをランダムに変更したりするなど、検出効率の差をキャンセルするメカニズムを採用することができる。これらの緩和メカニズムは物理的な手段を含むため、キャンセルはまだ不完全である。

If the TOE passes the functional test described in Subsubsection 10.9.2, the probability that the passive attack based on sifted key inference will succeed is expected to be extremely low, based on the rationale provided in Subsubsection 13.2.1. Therefore, the penetration test for this attack can be waived.
TOE が 10.9.2 項に記述された機能テストに合格した場合、13.2.1 項で説明された理由に基づき、シフト鍵の推論に基づくパッシブ攻撃が成功する確率は極めて低いと予想される。したがって、この攻撃に対する侵入テストは省略可能である。

9.2.2. Degrees of freedom

Description of assumption family:
An ideal detection unit reacts always in the same way irrespective of the degree of freedom into which the quantum signal is encoded. For polarization coding, for example, the detectors monitoring the various polarization modes are assumed to behave the same for all the pulses' degrees of freedom, such as timing, wavelength or spatial mode.
理想的な検出ユニットは、量子信号が符号化される自由度に関係なく、常に同じように反応する。例えば、偏光コーディングの場合、さまざまな偏光モードを監視する検出器は、タイミング、波長、空間モードなど、すべてのパルスの自由度に対して同じように動作すると想定される。
Description of the attack method:
The attacker modifies the degrees of freedom of the optical pulse on the quantum channel.
攻撃者は、量子チャネル上で、光パルスの自由度を改変する。
For example:

- delays the optical pulse;
- shifts wavelength phase of the optical pulse;

- shifts polarization of the optical pulse.

例えば：

- 光パルスを遅延する;
- 光パルスの波長をシフトする;
- 光パルスの偏光方向をシフトする。

If detection efficiency of the photon detector changes depending on these degrees of freedom, in the extreme case the QKD receiver will be unable to receive bit 0, the attacker can presume that all raw key is bit 1. Even if it is not so extreme, if detection efficiency for bit 0 of the detector decreases, the attacker can estimate with high probability that the raw key is bit 1.

これらの自由度に応じて単一光子検出器の検出効率が変化する場合、極端な例では、受信機はビット 0 を受信できなくなり、攻撃者はすべての生鍵がビット 1 であると推定できる。そこまで極端でなくとも、検出器のビット 0 の検出効率が低下すると、攻撃者は、高い確率で「生鍵はビット 1 である」と推定できる。

Assessment:

The degrees of freedom of light pulse include polarization, spatial mode, timing, and wavelength. However, since the spatial mode is defined by the input single-mode fibre and there is only one spatial mode incident on the photon detectors, it is impossible to attack using the difference in detection efficiency depending on the spatial mode.

光の自由度としては偏光、空間モード、時間、波長がある。但し、空間モードは入力のシングルモードファイバによって規定され、単一光子検出器に入射する空間モードは一つであるため、空間モードによる検出効率の違いを利用した攻撃は不可能である。

The time-shift attack, wavelength-dependent attack, and polarization--dependent attack described above can be performed with current technology. The penetration tests are described in Subsubsection 11.2.1 for the attacks. However, if the TOE passes the functional test described in Subsubsection 10.9.2, the probabilities that the TOE will not pass the penetration test for the time-shift attack is expected to be extremely low, based on the rationale provided in Subsubsection 13.2.1. Therefore, the penetration test for these attacks can be waived.

上記のタイムシフト攻撃、波長依存攻撃、偏波依存攻撃は現在の技術で実施可能である。侵入テストは、11.2.1 項に記述されている。ただし、TOE が 10.9.2 項に記述される機能テストに合格する場合、TOE がタイムシフト攻撃の侵入テストに合格しない確率は、13.2.1 項で示された理由に基づき、極めて低いと予想される。したがって、これらの攻撃に対する侵入テストは免除できる。

References:

B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, “Time-shift attack in practical quantum cryptosystems”, Quantum Inf. Comput. **7**, 73–82 (2007).

9.2.3. Security boundary on optical channel

Description of assumption family:

It is assumed that an ideal QKD transmitter allows no reading of its internal settings and no modification of its internal components.

理想的な QKD 受信機の内部設定を読み取ったり、内部コンポーネントを変更したりすることはできないと想定される。

Description of the attack method:

- An attacker reads/writes internal settings of the QKD receiver.

- An attacker modifies internal components of the QKD receiver.
- An attacker reads internal confidential data from internal components of the QKD receiver.
- An attacker observes internal states of the QKD receiver.

・ 攻撃者は、QKD 受信機の内部設定を読み書きする。
・ 攻撃者は、QKD 受信機の内部コンポーネントを変更する。
・ 攻撃者は、QKD 受信機の内部コンポーネントから、内部の秘密データを読み出す。
・ 攻撃者は、QKD 受信機の内部状態を観察する。

An attacker uses these adverse actions to disclose the QKD key or compromise the QKD receiver.
攻撃者はこれらの有害なアクションを使用して、QKD 鍵を暴露したり、QKD 受信機を危殆化したりする。

Assessment:

The security and cryptographic boundaries of the QKD receiver are physically protected due to the assumption of each PP. i.e. A.SecureOp of [PP-EAL4] or A.PHYSICAL of [PP-EAL2]. So an attacker cannot access internal components of the QKD receiver directly.
The internal settings of the QKD receiver are protected by user identification and authentication functions and access control functions via user interface(s). So an attacker cannot access internal settings of the QKD receiver via user interface(s).
If above assumptions are achieved and above functions are implemented completely and accurately, no potential vulnerabilities exist in above point of view.
QKD 受信機のセキュリティ暗号境界は、各 PP の前提条件によって、物理的に保護されている。つまり、[PP-EAL4]の A.SecureOp、または、[PP-EAL2]の A.PHYSICAL である。そのため、攻撃者は QKD 受信機の内部コンポーネントに直接アクセスできない。
QKD 受信機の内部設定は、利用者識別認証機能とアクセス制御機能によって保護されている。そのため、攻撃者は利用者インターフェースを介して QKD 受信機の内部設定にアクセスできない。
上記の前提条件が達成され、上記の機能が完全かつ正確に実装されているならば、上記の観点での潜在的脆弱性は存在しない。
However, the QKD link is not physically protected and not access controlled. An attacker may observe or modify internal state of the QKD receiver via the QKD link, e.g. choice of encoding basis.
しかし、QKD リンクは物理的に保護されておらず、アクセス制御もされていない。攻撃者は、QKD リンクを介して、QKD 受信機の内部状態を観察または改変する可能性がある。
The attack method that exploits modification of the internal state is used in some attacks. An example is bright illumination attack described in Subsubsection 9.2.5.
内部状態の改変を悪用する攻撃手法は、いくつかの攻撃で使われる。一つの例は 9.2.5 項で記述された Bright-Illumination Attack である。
One of attack method that exploits observation of the internal state is Back-flash attack. This attack is applicable when different detectors are implemented for each photon state. It is known that detectors emit weak light by themselves in response to detection. If the emission varies depending on detectors, an attacker can obtain information on detector detection events by observing the emission. The Back-flash attack can be performed with current technology. It is necessary to conduct and pass penetration tests. The penetration test for the attack is described in Subsubsection 11.2.2.
内部状態の観測を悪用する攻撃手法の 1 つはバックフラッシュ攻撃がある。この攻撃は、光子状態毎に異なる検出器が実装されている場合に適用できる。検出器は、検出に応じて自ら微弱に光発することが知られている。発光が検出器毎に異なるならば、攻撃者は、その発光を観察する事によって、検出器の検出イベントに関する情報

を取得できる。バックフラッシュ攻撃は現在の技術で実行可能である。侵入テストを実施し、合格する必要がある。攻撃に対する侵入テストは 11.2.2 項に記述されている。

Another attack method that exploits observation of the internal state is Trojan horse attack. This attack is applicable when the modulator is used to select the basis and same detector is used for all basis. An attacker injects light into the QKD receiver via the QKD link, observes the reflected light, and estimates the basis state.
内部状態の観測を悪用するもう 1 つの攻撃手法は、トロイの木馬攻撃である。この攻撃は、変調器を使用して基底を選択し、全ての基底に同じ検出器を使用する場合に適用できる。攻撃者は、QKD リンクを介して受信機に光を注入し、反射光を観測して基底状態を推定する。

Trojan horse attack countermeasures are implemented in several steps.
1. A light injection monitor is implemented that monitors the light intensity injected into the QKD receiver.
2. When the light injection monitor detects strong light, the TSF will automatically respond to prevent information leakage due to light reflection. e.g. the TSF performs "emergency stop of the QKD link" (FPT_PHP.3).
3. When light is injected below the detection limit, the maximum reflected light intensity is estimated based on the transmission and reflection characteristics of the QKD receiver components.

トロイの木馬攻撃の対抗策は、いくつかのステップで実装される。
1. 受信機に注入される光強度を監視する光注入モニタが実装される。
2. 光注入モニタが強い光を検知すると、TSF は自動的に応答し、光の反射による情報漏洩を防ぐ。例えば TSF は、「QKD リンクの緊急停止」を実行する(FPT_PHP.3)。
3. 検出限界以下の光が注入された場合、最大反射光強度は、受信機コンポーネントの透過特性と反射特性に基づいて推定される。

If the security proof specifies quantitative assumptions on the reflected light intensity and those assumptions can be verified by functional testing, no further analysis is required on the Trojan horse attack.
セキュリティ証明が反射光の強度に関する定量的な想定を規定しており、その想定が機能テストで検証できる場合は、トロイの木馬攻撃に関するさらなる分析は必要ない。

If it is not the case, assessment of vulnerabilities against the Trojan horse attack is necessary, which is as follows.
The Trojan horse attack can be performed with current technology. It is necessary to conduct and pass penetration tests. The penetration test for the attack is described in Subsubsection 11.2.2.
そうでない場合は、上記の攻撃に対する次のような脆弱性の評価が必要である。
トロイの木馬攻撃は現在の技術で実行可能である。侵入テストを実施し、合格する必要がある。攻撃に対する侵入テストは 11.2.2 項に記述されている。

9.2.4. Accuracy of the demodulation

Description of assumption family:

The decoy-state BB84 protocol dictates that the receiver chooses between the two measurement bases. A measurement basis is usually determined by a set of optical components in front of two photon detectors. An ideal receiver can perfectly distinguish the two optical modes used for encoding on the chosen basis.
decoy-state BB84 プロトコルは、受信機が 2 つの測定基底のうちひとつを選択することを要求する。通常、測定

基底は、2つの光子検出器の手前に置かれた1組の光学素子によって決定される。理想的な受信機は、選択した基底の符号化に用いられる2つの光学モードを完全に弁別できる。

Description of the attack method:

Intercept-resend attack on the monitoring basis: The attacker intercepts the encoded pulse(s) from the QKD transmitter and makes a photon detection to distinguish the two states for the basis used for monitoring, determining a bit value. When the detection was successful, the attacker prepares a stronger optical pulse with the proper modulation corresponding to the determined bit value and sends it to the QKD receiver. This attack introduces no additional errors, but the determined bit value may partially reveal the bit value determined by the QKD receiver on the other basis if the measurement bases are not accurate.

監視用基底への Intercept-resend 攻撃：攻撃者は、QKD 送信機からの符号化パルスを傍受し、監視に使用される基底に対して2つの状態を区別する光子検出を行い、ビット値を決定する。検出が成功すると、攻撃者は決定されたビット値に対応する適切な変調を施したより強力な光パルスを準備し、それを QKD 受信機に送信する。この攻撃によって新たなエラーが生じることはないが、測定基底が正確でない場合、決定されたビット値によって、もう一方の基底で QKD 受信機が決定したビット値が部分的に明らかになる可能性がある。

Assessment:

If the security proof makes no assumption on the accuracy of measurement bases, or if it specifies relevant quantitative assumptions and those assumptions can be verified by functional testing, no further analysis is required. If it is not the case, assessment of vulnerabilities against the attack described above is necessary, which is detailed in the following.

セキュリティ証明が測定基底の正確性についての仮定を用いていないか、あるいは、関連する定量的な仮定が指定され、その仮定が機能テストによって検証できる場合、それ以上の分析は必要ない。

そうでない場合は、上記の攻撃に対する脆弱性の評価が必要であり、その評価は以下に詳細化する。

The intercept-resend attack on the monitoring basis can be performed with current technology. It is necessary to conduct and pass penetration tests. The penetration test for the attack is described in Subsubsection 11.2.4.

監視用基底への Intercept-resend 攻撃は現在の技術で実行可能である。侵入テストを実施し、合格する必要がある。攻撃に対する侵入テストは 11.2.4 項に記述されている。

9.2.5. Single-photon sensitivity

Description of assumption family:

It is assumed that the single photon sensitivity of the QKD receiver is not controlled by injected bright light.

受信機の単一光子感度は、注入された明るい光によって制御される事はないと想定される。

Description of the attack method:

An attacker injects bright light to the QKD receiver at the timing when the light pulse of the QKD transmitter should be received. After that, the attacker injects trigger light that encodes his own bit values. If the detection efficiency of the single photon detector in the QKD receiver decreases due to the injected bright light, the QKD receiver will not be able to receive the photons transmitted by the QKD transmitter. In this situation, the attacker can force to receive intended bit value to the QKD receiver using own trigger light at a later timing.

攻撃者は、送信機の光パルスを受信すべきタイミングで受信機に明るい光を注入する。 その後、攻撃者は自分のビット値をエンコードしたトリガ光を注入する。明るい光が注入されて受信機の単一光子検出器の検出効率が低

下すると、受信機は送信機から送信された光子を受信できなくなる。この状況では、攻撃者は、その後のタイミングで、自身のトリガ光を使って、受信機に意図したビット値を強制的に受信させることができる。

There are two distinct types of bright illumination attacks. In the ideal case, those attacks are described as follows. (Here we assume a decoy state BB84 protocol in which the sifted key is generated from the Z basis only and the X basis is only used to monitor eavesdropping.)

明光攻撃には 2 つのタイプがある。理想的な場合、これらの攻撃は以下のように記述される。(ここでは、シフト鍵が Z 基底のみから生成され、X 基底は盗聴の監視にのみ使用される、decoy state BB84 プロトコルを仮定する)

1). Bright light puts all detectors in linear mode. When a strong control light with the same optical mode as a signal light used in the Z-basis is injected, all the light in the Z-basis is incident on the corresponding detector. The intensity of the control light is chosen so that the intensity at the incidence is slightly above the threshold of the linear mode detector. In this case, no detection occurs in the X-basis, as the control light is equally divided between the two detectors.

   明光により、すべての検出器をリニアモードにする。 Z 基底の信号光と同じ光学モードを持つ強い制御光を入射すると、Z 基底では特定の検出器にすべての光が入射する。この時の入射強度がリニアモード検出器のしきい値より少し上になるように制御光の強度を選ぶ。この時、X 基底では 2 つの検出器に等分されて入射するため、検出が起こらない。

2). This attack is only valid for devices with passive base selection. The passive basis selection device uses a pair of photon detectors for the measurement of the X-basis and a pair of photon detectors for the measurement of the Z-basis. Bright light reduces only the quantum efficiency of the detectors in the X-basis to zero. When the control light with the same mode as a signal light used in the Z-basis is injected, all the light branched to the Z-basis detection is incident on the corresponding detector and only that detector causes detection. The X-basis detectors do not cause detection due to the bright light.

   この攻撃は受動基底選択の装置にのみ有効である。受動基底選択の装置は、X 基底の測定用に 1 対の単一光子検出器が、Z 基底の測定用に 1 対の単一光子検出器が用いられる。明光により、X 基底の検出器の量子効率だけをゼロにする。Z 基底の信号光と同じモードを持つ制御光を入射すると、Z 基底では特定の検出器にすべての光が入射し、その検出器のみが検出を起こす。X 基底の検出器は明光の影響で検出を起こさない。

By using attack type 1) or 2) at the resending step of the intercept-resend attack, the attacker can learn the value of the sifted key in the Z basis without increasing the bit error in the X basis.

攻撃タイプ 1)または 2)を、Intercept-resend 攻撃の resend 時に用いることで、攻撃者は X 基底のビットエラーを上昇させずに Z 基底のシフト鍵の値を知ることができる。

Assessment:

One of countermeasure against bright-illumination attack is to implement a light injection monitor in the TOE. The light injection monitor is a function implemented inside the QKD receiver, which detects and alarms when bright light is input. If no countermeasures are implemented, FPT_PHP.3 is not fulfilled, and ADV activity of the evaluation will be failed. Based on the rationale provided below, a set of the functional tests in Subsection 10.3.3.5 and Subsubsection 10.9.2.1, instead of a penetration test, can suffice to evaluate how well the TOE withstand bright-illumination attacks.

明光攻撃に対するひとつの対抗策は、光注入モニタの TOE への実装である。光注入モニタは、QKD 受信機の内部に実装されている機能であり明るい光が入力された場合にはそれを検出してアラームを通知する。もし、何の対抗策も実装されてなければ、FPT_PHP.3 は満たされず、その評価の ADV アクティビティは FAIL する。下記に示す根拠に基づき、侵入テストの代わりに、10.3.3.5 節および 10.9.2.1 に記載されている一連の機能テストに

よって、TOE が明光攻撃にどれだけ耐えられるかを評価することができる。

Feasibility of attack type 1) can be evaluated from the functional test in Subsubsection 10.9.2.1. When a detector goes to the linear mode under illumination of a bright pulse with an intensity μ, it is no longer sensitive to a small signal input. It follows that if the intensity of the bright pulse is increased from zero to μ, a significant decrease of sensitivity to a small signal input should be observed. On the other hand, the functional test requires that there be no loss of sensitivity in the intensity range at which the light injection monitor is not activated. Hence, if the TOE passed the functional test of Subsubsection 10.9.2.1, the attack type 1) should fail because it is impossible to make the detectors transition to the linear mode without triggering the light injection monitor.
攻撃タイプ 1）のフィージビリティは、10.9.2.1 項の機能テストから評価できる。強度μの明光の入射で検出器がリニアモードになるとき、小信号入力に対する感度は失われている。そのため、明光の強度をゼロから μ へと変化させた時、小信号入力に対するはっきりした感度の低下が観測されるはずである。一方、機能テストは、光注入モニタが作動しない強度範囲で感度の低下がないことを要求している。従って、10.9.2.1 項の機能テストに合格した TOE に対しては、その光注入モニタを作動させることなしに検出器をリニアモードに移行させることができないため、タイプ 1)の攻撃は失敗するはずである。
The attack type 2) may still effective even if the detectors are not switched to the linear mode. This attack can be performed with current technology, and the penetration tests described in Subsubsection 11.2.3 can be identified for the attack. However, if the TOE passes the functional test described in Subsubsection 10.9.2.1, the probability that the TOE will not pass the penetration test described in Subsubsection 11.2.3 is expected to be extremely low, based on the rationale provided in Subsubsection 13.2.2.
攻撃タイプ 2)は、検知器がリニアモードに切り替えられなくても有効である。この攻撃は現在の技術で実行可能であり、11.2.3 項で説明される侵入テストはこの攻撃に対して識別可能である。ただし、TOE が 10.9.2.1 項に記述されている機能テストに合格している場合、11.2.3 項で説明されている侵入テストに TOE が合格しない確率は、13.2.2 項で示された理由に基づき、極めて低いものと予想される。

References:

L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, “Hacking commercial quantum cryptography systems by tailored bright illumination”, Nat. Photonics 4, 686–689 (2010).
L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, “Thermal blinding of gated detectors in quantum cryptography”, Opt. Express 18, 27938 (2010).
C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, “After-gate attack on a quantum cryptosystem”, New J. Phys. 13, 013043 (2011).
L. Lydersen, N. Jain, C. Wittmann, Ø. Marøy, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, “Superlinear threshold detectors in quantum cryptography”, Phys. Rev. A84, 032320 (2011).

9.2.6. Recovery or dead time

Description of assumption family:

It is assumed that detection efficiency of the photon detector is not affected by past detection events.
This assumption can be seen as a subset of the assumption on single photon sensitivity. After a detection event, a single photon detector takes some time to recover (referred to as dead-time). During this time, it loses its single photon sensitivity.
単一光子検出器の検出効率は前の検出イベントの影響を受けないと想定される。

この仮定は、単一光子感度に関する仮定のサブセットと見なすことができる。検出イベントの後、単一光子検出器が回復するのに少し時間がかかる（デッドタイムとして参照される)。この間、単一光子の感度が失われる。

Description of the attack method:

An attacker injects blinding light to the QKD receiver outside the detection window of the QKD receiver and aiming at the timing when the transmitted pulse arrives in the dead-time of the detector. The timing should be a little before the detection window.

If the blinding light is encoded a specific photon state used in the TOE, the light blinds a specific photon detector. For example, when the blind light is encoded bit “1” with Z-basis , the QKD receiver will not be able to receive bit “1” with Z-base. As a result, the bit "1" is lost with in Z-basis, and an attacker can predict that the bit in the sifted key is "0" with high probability.

Experiments show that this attack is successful even with blind light of 20 photons or less.

攻撃者は、送信パルスが検出器のデッドタイムに到達するタイミングを狙って、受信機の検出ウィンドゥの外で受信機にブラインド光を注入する。そのタイミングは検出ウィンドウの少し前になるはずである。

TOE で使用される特定の光子状態がブラインド光にエンコードされている場合、その光は特定の単一光子検出器をブラインドする。たとえば、そのブラインド光が Z 基底でビット”1”にエンコードされている場合、受信機は Z 基底でビット”1”を受信できなくなる。その結果、ビット”1”が失われ、攻撃者は、高い確率でシフト鍵のビットは”0”であると予測できる。

実験では、この攻撃は 20 光子以下のブラインド光でも成功することが示されている。

Assessment:

Some TOEs implement countermeasures to ensure that the photon detector is not blinded.

For Example,

(a) The QKD receiver monitors the terminal voltage of the detector. Since the terminal voltage is temporarily dropped due to photo detection, if a terminal voltage of one detector drops, the QKD receiver disables all detections until the terminal voltage recovers.

(b) If a gated mode photon detectors are implemented, the QKD receiver controls the gate signal to not detect photons before the detection window.

いくつかの TOE 実装によっては、単一光子検出器がブラインドされない事を保証する対策が実装される場合がある。

a) 受信機は検出器の端子電圧を監視する。光検出により端子電圧は一時的に低下するため、1 つの検出器の端子電圧が低下したならば、受信機はその端子電圧が回復するまで、全ての検出を無効化する。

b) ゲートモード単一光子検出器が実装されている場合、受信機は、検出ウィンドウの前に光子を検出しないようにゲート信号を制御する。

However, even if (a) is implemented, the terminal voltage drop width and the dead-time width may not be exactly same. The time of descent may be shorter than the dead time, and the detector may be activated during the dead time.

If (b) is implemented, an attacker may inject strong blind light to force detection and blind the detector. To counter such attacks, light monitors can also be implemented to detect the stronger light. However, the sensitivity of the light monitor may not be sufficient to detect the blind light and fail to prevent blinding.

Therefore, the penetration tests shall demonstrate the TOE counters such attacks. See Subsubsection 11.2.5.

しかし(a)が実装された場合でも、端子電圧における降下時間幅とデッドタイム幅は完全に一致しないかも知れない。降下時間幅がデッドタイム幅より短い場合があり、デッドタイムの間に検出器が有効化される場合がある。

(b)が実装された場合でも、攻撃者が強いブラインド光を注入すると、その光が検出を強制し、検出器をブライン

ドするかも知れない。このような攻撃に対抗するために、より光を検出する為の光モニタも実装されるかも知れないが、光モニタの感度はブラインド光を検出十分でないかも知れず，ブラインドされることを防げないかもしれない。
それゆえ、侵入テストは、TOE がそのような攻撃に対抗することを実証しなければならない。11.2.5 項を参照のこと。

References:

H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, “Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors”, New J. Phys. **13**, 073024 (2011).

9.3. Whole of the TOE

9.3.1. Calibration

Description of assumption family:

It is commonly assumed that the optical signals exchanged in the calibration phase cannot be exploited by the attacker to enhance her attack against the QKD system. However, a slack execution of these phases, lacking coordination between the users or leaking more information than strictly necessary to the eavesdropper can compromise the security of the whole QKD system.
キャリブレーションフェーズで交換された光信号は、QKD システムに対する攻撃を強化するために攻撃者が利用することはできないと一般に想定されている。ただし、これらのフェーズの実行が遅れたり、ユーザー間の調整が不足したり、盗聴者に厳密に必要な以上の情報が漏洩したりすると、QKD システム全体のセキュリティが危険にさらされる可能性がある。

Description of the attack method:

For example, if the QKD receiver uses two detectors, the detection timing is adjusted using two pulses, one to adjust the detection timing of detector-A and the other to adjust the detection timing of detector-B. An attacker imposes a time delay only on the training pulse for detector-A. Then the detector-A is adjusted to non-optimal detection timing. If this reduces the detection efficiency of the detector-A, an attacker may succeed in the detection efficiency mismatch attack shown in Subsubsection 9.2.1.
例えば、受信機が 2 つの検出器を使用している場合、検出タイミングは 2 つのパルスを使用して調整される。1 つは検出器 A の検出タイミングを調整し、もう 1 つは検出器 B の検出タイミングを調整する。攻撃者は、検出器 A の調整パルスにのみ時間遅延を適用する。すると、検出器 A は非最適な検出タイミングに調整される。これにより検出器 A の検出効率が低下すると、攻撃者は 9.2.1 項に示す検出効率不一致攻撃に成功する可能性がある。

Assessment:

The penetration tests shall demonstrate the TOE counters such attacks. See Subsubsection 11.3.1.
侵入テストは、TOE がそのような攻撃に対抗することを実証しなければならない。11.3.1 項を参照のこと。

9.3.2. Stabilities of the light source and the photon detector

Description of assumption family:

The light source of the QKD transmitter and the photon detectors of the QKD receiver are typically assumed to be stable and the characteristics are the same as when they were characterised. However, in practice, the light source and the photon detector may deteriorate over time and the security of the TOE cannot be guaranteed with the deteriorated characteristics of the device.

受信機 QKD 送信機の光源と QKD 受信機の単一光子検出器は通常、安定しており、特性は評価が行われたときと同じであると想定される。しかし、実際には、光源と単一光子検出器は時間とともに劣化するため、TOE の安全性は劣化したデバイス特性では保証できない可能性がある。

Description of the attack method:

If the light source of the QKD transmitter deteriorates over time, in extreme cases, the optical phase will become skewed, making it easier for attackers to predict the transmitted optical phase.

If the photon detector in the QKD receiver deteriorates over time, in an extreme case, the QKD receiver will be unable to receive bit 0, the attacker can estimate that all raw key is bits 1. Even if it is not so extreme, if detection efficiency for bit 0 of the detector decreases, the attacker can estimate with high probability that the raw key is bit 1.

QKD 送信機の光源が経年劣化した場合、極端な例では、光位相が偏り、攻撃者は送信された位相を予想しやすくなる。受信機の単一光子検出器が経年劣化した場合、極端な例では、受信機はビット 0 を受信できなくなり、攻撃者はすべての生鍵がビット 1 であると推定できる。そこまで極端でなくとも、単一光子検出器のビット 0 の検出効率が低下すると、攻撃者は、高い確率で「生鍵はビット 1 である」と推定できる。

Assessment:

The developer shall provide a routine inspection measure to ensure that the light source of the QKD transmitter and the photon detectors in the QKD receiver is no performance degradation for the TOE user. If the performance of the light source and photon detector are maintained through the regular inspection, penetration tests are not necessary.

開発者は、QKD 送信機の光源と QKD 受信機の単一光子検出器に性能劣化がないことを確認するための定期的な検査手段を、TOE 利用者に提供しなければならない。定期的な検査手段により光源と単一光子検出器の性能が維持されていれば、侵入テストは必要ない。

9.3.3. Robustness against provoked damage

Description of assumption:

It is assumed that the light source of the QKD transmitter and the photon detectors in the QKD receiver works properly.

QKD 送信機内の光源と QKD 受信機内の単一光子光子検出器が正しく動作すると想定される。

Description of the attack method:

An attacker injects strong light to the QKD receiver or the QKD transmitter via the quantum channel.

If the photon detector for bit 0 in the QKD receiver is permanently damaged due to the attack, in an extreme case, the QKD receiver will be unable to receive bit 0, the attacker can estimate that all sifted key is bits 1. Even if it is not so extreme, if detection efficiency for bit 0 of the detector decreases, the attacker can estimate with high probability that the sifted key is bit 1. If the modulator in the QKD transmitter is permanently damaged due to the attack, in an extreme case, only the unmodulated state is sent from the QKD transmitter. The attacker predicts the bit values in the sifted key with a high probability.

攻撃者は、量子チャネルを介して受信機または送信機に強い光を注入する。

攻撃によって受信機のビット 0 用の単一光子光子検出器が恒久的に損傷した場合、極端な例では、受信機はビット 0 を受信できなくなり、攻撃者はすべてのシフト鍵がビット 1 であると推定できる。そこまで極端でなくとも、検出器のビット 0 の検出効率が低下すると、攻撃者は、高い確率で「シフト鍵はビット 1 である」と推定で

きる。もし，送信機の変調器が恒久的に損傷した場合、極端な例では、変調していない状態のみが送信される．攻撃者は高い確率でシフト鍵のビット値を推定できる。

Assessment:

No countermeasures are currently known to completely prevent damage to the optical devices.
Theoretically, for example after injecting very strong light into the QKD receiver, a penetration test can be considered that demonstrates that there is no significant difference in the detection efficiency of bit 0 and bit 1, but this test means a fracture test. Therefore, it is difficult to ensure that the TOE counters this attack method completely.
At the least, the developer shall provide a routine inspection measure to ensure that the optical devices in the QKD transmitter and QKD receiver is undamaged for the TOE user. If the performance of the light source and photon detector are maintained through the regular inspection, penetration tests are not necessary.
現状、光素子の損傷を完全に防ぐ対抗策は知られていない。
理論的には、例えば、受信機に非常に強い光を注入した後、ビット 0 とビット 1 の検出効率に有意差がないことを示す侵入テストが考えられるが、このテストは破壊テストを意味する。従って、TOE がこの攻撃方法に完全に対抗することを保証することは困難である。
少なくとも、開発者は、QKD 送信機と QKD 受信機の光素子に損傷がないことを確認するための定期的な検査手段を、TOE 利用者に提供しなければならない。定期的な検査手段により光源と単一光子検出器の性能が維持されていれば、侵入テストは必要ない。

9.3.4. Authenticated classical channel

Description of assumption:

The authenticated classic channel is assumed to assure the identification of the endpoint that sent the channel data and to protect the integrity of the channel data.
認証済み古典チャネルは、チャネルデータを送信したエンドポイントの識別を保証し、及びチャネルデータの完全性を保護することを想定している。

Description of the attack method:

There are various methods of attack for authenticated classical channel. For example, an attacker could install a packet sniffer on the classical communication channel between the QKD transmitter and the QKD receiver, and then impersonate the QKD transmitter and QKD receiver to eavesdrop on or tamper with the communication content.
認証済み古典チャネルにおいては、様々な攻撃の方法がある。例えば、攻撃者が QKD 送信機と QKD 受信機の間の古典通信路にパケットスニッファーを設置し、QKD 送信機・QKD 受信機になりすまして通信内容を盗聴したり改ざんしたりする。

Assessment:

The penetration tests shall demonstrate the TOE counters such attacks. For [PP-EAL4] and [PP-EAL2], the protocol to be implemented in the authenticated classical channel is not specified, and the TOE developer decides the protocol. The evaluator shall search for vulnerabilities in the implemented protocols and conduct penetration tests in accordance with [CEM].
侵入テストは、TOE がそのような攻撃に対抗することを実証しなければならない。[PP-EAL4]と[PP-EAL2]では認証済み古典チャネルに実装するプロトコルは決められておらず、TOE 開発者がプロトコルを決定する。評

価者は[CEM]に従い、実装されているプロトコルの脆弱性を探査し、侵入テストを実施しなければならない。

9.3.5. Random number generators

Description of assumption:

It assumed that the random number generator provides random bits that meets the defined quality metric.
乱数生成器は定義された品質に合致するランダムビットを供給すると想定されている。

Description of the attack method:

- An attacker reads raw random bits from internal components of the QKD receiver or the QKD transmitter.
- An attacker modifies raw random bits in internal components of the QKD receiver or the QKD transmitter.
- An attacker reads digitized random numbers from internal components of the QKD receiver or the QKD transmitter.
- An attacker modifies digitized random numbers in internal components of the QKD receiver or the QKD transmitter.

・ 攻撃者は、QKD 受信機または QKD 送信機の内部コンポーネントから生のランダムビットを読み出す。
・ 攻撃者は、QKD 受信機または QKD 送信機の内部コンポーネント内の生のランダムビットを変更する。
・ 攻撃者は、QKD 受信機または QKD 送信機の内部コンポーネントからデジタル化した乱数を読み出す。
・ 攻撃者は、QKD 受信機または QKD 送信機の内部コンポーネント内のデジタル化した乱数を変更する。

An attacker uses these adverse actions to compromise the QKD receiver or the QKD transmitter.
攻撃者はこれらの有害なアクションを使用して、QKD 受信機または QKD 送信機を危殆化する。

Assessment:

The QKD receiver and the QKD transmitter are physically protected due to the assumption of each PP. i.e. A.SecureOp of [PP-EAL4] or A.PHYSICAL of [PP-EAL2]. So an attacker cannot access internal components of the QKD receiver or the QKD transmitter directly.
If above assumptions are achieved, no potential vulnerabilities exist in above point of view.
QKD 受信機と QKD 送信機は、各 PP の前提条件によって、物理的に保護されている。すなわち、[PP-EAL4] の A.SecureOp、または、[PP-EAL2]の A.PHYSICAL である。そのため、攻撃者は QKD 受信機または QKD 送信機の内部コンポーネントに直接アクセスできない。
上記の前提条件が達成されているならば、上記の観点での潜在的脆弱性は存在しない。

10. Functional Tests

This section describes the functional tests that developer shall conduct. The functional tests described here have been deemed necessary by experts in the context of the related SFRs for testing upon the TOE. Additionally, functional tests that are required to be conducted in the process of identifying vulnerabilities in Section 9 are outlined in Subsection 10.9. The evaluator examines that the developer conducted the functional tests in this section according to the evaluation activity in Subsection 8.5.
本章では、開発者が実施しなければならない機能テストを記述する。ここで記述されている機能テストは、関連する SFR の文脈で TOE におけるテストが必要であると専門家が判断したものである。さらに、9 章の脆弱性を識別する過程において実施することを求められている機能テストは、10.9 節に規程されている。評価者は、8.5 節の評価アクティビティに従い、開発者がこの章の機能テストを実施したことを検査する。

10.1. FCS_QKD.1

Test 1:

This test demonstrates the establishment of identical QKD keys according to the QKD protocol (FCS_QKD.1.1).
このテストは、QKD プロトコルに従った同一の QKD 鍵の確立を実証する(FCS_QKD.1.1)。

Step 1. The tester shall start QKD session.
試験者は QKD セッションを開始しなければならない。

Step 2. The tester shall continue the QKD session until 200,000 bits or more QKD keys are established.
試験者は、200,000 ビット以上の QKD 鍵が確立されるまで QKD セッションを継続しなければならない。

Step 3. The tester shall retrieve the QKD keys from the QKD transmitter and the QKD receiver.
試験者は、送信機と受信機から QKD 鍵を取得しなければならない。

Step 4. The tester shall compare the QKD keys retrieved from the QKD transmitter and the QKD keys retrieved from the QKD receiver.
試験者は、送信機から取得した QKD 鍵と受信機から取得した QKD 鍵を比較しなければならない。

Step 5. If the QKD keys match, the test result is PASS, otherwise the test result is FAIL.
QKD 鍵が一致する場合、テスト結果は PASS であり、そうでなければテスト結果は FAIL である。

Test 2:

The developer shall demonstrate that post-processing consistent with the functional specification is correctly implemented based on each post-processing algorithm assigned to FCS_QKD.1.4 and each privacy amplification algorithm assigned to FCS_QKD.1.6. Actual functional tests depend on the assignment of the SFR and description of the functional specification. The functional tests might be as follows in a typical case where the raw key are sequentially converted to sifted key through a sifting scheme, to reconciled key through error correction scheme, and then to QKD keys through a privacy amplification scheme.
開発者は、機能仕様と一貫した後処理が、FCS_QKD.1.4 に割付けられたそれぞれの後処理アルゴリズムと FCS_QKD.1.6 に割付けられたそれぞれの秘匿性増強アルゴリズムに基づいて正しく実装されていることを実証しなければならない。実際の機能テストは SFR の割付けと機能仕様の記述によって異なる。生鍵が逐次、ふるい分けスキームによってふるい鍵に、誤り訂正スキームによって訂正済み鍵に、さらに秘匿性増強スキームによって QKD 鍵に変換されるという典型的な場合には、機能テストは以下の様になるだろう。

Step 1. Sifting scheme

The correctness of the implementation of this scheme shall be demonstrated by verifying that bits whose basis does not match are removed after sifting for raw key.

ふるい分けスキーム

このスキームの実装の正しさは、一致しない基底選択によって生成された生鍵内のビットが、ふるいにかけられたビット列から削除されていることによって実証しなければならない。

Step 2. Error correction scheme

The correctness of the implementation of this scheme shall be demonstrated by verifying that the erroneous bits are corrected after error correction under situation where the communication errors of basis-matched raw key occur. Note that too many errors may cause the QKD session to be re-executed based on FCS_QKD.1.2, making it impossible to observe error correction behaviour. The error correction scheme may be followed by a process of the consistency check of the pair of the reconciled key. In such a case, the correctness of the implementation of the consistency check shall be demonstrated by verifying that the same hash value is obtained when the same string is input into the implemented hash function and that different hash values are obtained when different strings are input.

誤り訂正スキーム

このスキームの実装の正しさは、基底が一致した生鍵における通信エラーが発生した場合に、誤り訂正された後に誤ったビットが修正されることを検証することによって実証しなければならない。エラーが多すぎると FCS_QKD.1.2 に基づいて QKD セッションが再実行され、誤り訂正のふるまいを観察できなくなる可能性があることに注意する。誤り訂正スキームが、訂正済み鍵対の一貫性を確認するプロセスに続いて行われる場合がある。その場合、一貫性チェックの実装の正確性は、実装されているハッシュ関数に同じ系列を入力した際には同じハッシュ値が得られ、異なる系列を入力した際には異なるハッシュ値が得られることを検証することによって実証しなければならない。

Step 3. Privacy amplification scheme

The correctness of the implementation of this scheme shall be demonstrated by verifying that the reconciled key is shortened by privacy amplification according to the privacy amplification ratio that is deduced based on FCS_QKD.1.5.

秘匿性増強スキーム

このスキームの実装の正しさは、秘匿性増強によって訂正済み鍵が、FCS_QKD.1.5 に基づいて導出された秘匿性増強率に従って短縮されていることを確認することによって実証しなければならない。

Test 3: This test demonstrates the function of repeated executions of key establishment by the QKD protocol and the behaviour of the attempt counter for all attempts for key establishment (FCS_QKD.1.2).

このテストは QKD プロトコルによる鍵確立の繰り返し実行機能と鍵確立のための全試行についての試行カウンタのふるまいを実証する(FCS_QKD.1.2)。

Step 1. The tester shall query the key establishment attempt counter and record the value.

試験者は、試行カウンタを問合せ、値を記録しなければならない。

Step 2. The tester shall start QKD session and attempt the key establishment multiple times.

試験者は、QKD セッションを開始し、鍵の確立を複数回試行しなければならない。

Step 3. The tester shall stop QKD session after the key is established.

鍵が確立された後、試験者は QKD セッションを停止しなければならない。

Step 4. The tester ensure that value of the attempt counter is incremented by the count of attempts.

試験者は、試行カウンタの値が試行回数だけ増加することを確認しなければならない。

Step 5. If the value of the attempt counter is incorrect, the test result is FAIL, otherwise proceed to the next step.
試行カウンタの値が正しくない場合、テスト結果は FAIL であり、それ以外の場合は、次の手順に進む。

Step 6. If the TSF supports the function of automatic repeated executions of key establishment if the QKD protocol is aborted or sufficient key length is not established, the tester shall also perform the following steps:
QKD プロトコルが中止された場合、または十分な鍵長が確立されていない場合に、TSF が自動的な鍵確立の繰り返しをサポートする場合、試験者は以下の手順も実行しなければならない。

Step 7. The tester shall configure conditions in which repeated executions of key establishment are required. In order to support this step, the developer may provide a test function dedicated to fulfilling the condition. For example, the TOE forces to abort the first key establishment attempt.
試験者は、鍵確立の繰り返し実行が必要とされる条件を設定しなければならない。この手順を支援する為に、開発者は、条件を満たすためのテスト専用機能を提供してもよい。例えば、TOE は、最初の鍵確立の試行を強制的に中止するなど。

Step 8. The tester shall start QKD session and attempt the key establishment.
試験者は、QKD セッションを開始し、鍵確立を試みなければならない。

Step 9. The tester shall stop QKD session after the key is established.
鍵が確立された後、試験者は QKD セッションを停止しなければならない。

Step 10. The tester ensure that value of the attempt counter is added by automatically repetitions count.
試験者は、試行カウンタの値が自動的な繰り返し回数分、加算されることを確認しなければならない。

Step 11. The tester shall iterate step 7 to 10 until all the conditions in which repeated executions of key establishment are required are covered.
試験者は、鍵確立の繰り返し実行が必要とされるす全ての条件を網羅するまで、ステップ 7 から 10 を繰り返し実行しなければならない。

Step 12. For all iterations, if the value of the attempt counter is correct, the test result is PASS, otherwise the test result is FAIL.
全ての繰り返しに対して試行カウンタの値が正しい場合、テスト結果は PASS であり、それ以外の場合は、テスト結果は FAIL である。

Test 4:

This test demonstrates the behaviour of the FCS_QKD.1.2 functionality when the threshold of the attempt counter is exceeded.

このテストは FCS_QKD.1.2 の機能性である試行カウンタの閾値を超えたときのふるまいを実証する。

If the TOE does not support the management function that modifies threshold of the attempt counter, in order to support this test, the developer shall provide a test-dedicated interface to force any value to the threshold of the attempt counter.

TOE が試行カウンタの閾値を変更する管理機能をサポートしていない場合、このテストをサポートするために、開発者は、試行カウンタの閾値に任意の値を強制するためのテスト専用のインターフェースを提供しなければならない。

Step 1. The tester shall modify the threshold of the attempt counter to lower value. If multiple QKD key establishments are performed in parallel within one QKD session, the threshold value shall be set such that the attempt counter reaches the threshold plus one when below all QKD key establishments fail.
試験者は、試行カウンタのしきい値を小さな値に変更しなければならない。複数の QKD 鍵確立が 1 つ

の QKD セッション内で並行して実行される場合、しきい値は、下記の全ての QKD 鍵確立が失敗したときに試行カウンタがしきい値に 1 を加えた値に達するように設定されなければならない。

Step 2. The tester shall start QKD session.
試験者は、QKD セッションを開始しなければならない。

Step 3. The tester shall force to fail key establishment and repeat key establishment until the attempt counter reaches the threshold plus one.
試験者は、鍵の確立を強制的に失敗させ、試行カウンタがしきい値＋ 1 に達するまで鍵の確立を繰り返えさなければならない。

Step 4. The tester shall ensure that the QKD protocol execution is no longer allowed.
試験者は、QKD プロトコルの実行が許可されなくなったことを確認しなければならない。

Step 5. If the QKD protocol execution is denied, the test result is PASS, otherwise the test result is FAIL.
QKD プロトコルの実行が拒否された場合、テスト結果は PASS であり、それ以外の場合、テスト結果は FAIL である。

10.2. FPT_ITQ.1

Test 1: This test demonstrates the behaviour of the authenticated classical channel (FPT_ITQ.1).
このテストは認証済み古典チャネルのふるまいを実証する(FPT_ITQ.1)。

Step 1. The tester shall start QKD session.
試験者は QKD セッションを開始しなければならない。

Step 2. The tester shall modify information to be protected on the classical channel during the QKD session.
試験者は、QKD セッション中に古典チャネル上で保護されるべき情報を改変しなければならない。

Step 3. The tester shall ensure the TSF detects the modification and takes action after detection to be implemented.
試験者は、TSF がその改変を検出し、実装すべき検出後のアクションを実行することを確認しなければならない。

Step 4. The tester shall iterate step 1 to 3 until all information to be protected, such as bases information and error correction information are covered. For example, exchanging bases and exchanging error correction information. If the information is transmitted in both directions, the integrity check of the QKD transmitter and the integrity check of the QKD receiver shall be tested respectively.
試験者は、基底情報と誤り訂正情報のような保護されるべきすべての情報がカバーされるまで、ステップ 1 から 3 を繰り返さなければならない。例えば、基底の交換と誤り訂正情報の交換などである。情報が双方向で伝達されるならば、送信機の完全性チェックと受信機の完全性チェックは、それぞれテストされなければならない。

Step 5. For all iterations, if the action is consistent to the functional specification or the TOE design, the test result is PASS, otherwise the test result is FAIL.
全ての繰り返しに対してアクションが機能仕様または TOE 設計と一貫している場合、テスト結果は PASS であり、それ以外の場合、テスト結果は FAIL である。

10.3. FPT_EMS.1

10.3.1.Overview of functional tests of assumption families

If the assumption in the security proof is described with the values of realistic characteristics, the corresponding

values of the testable parameters/characteristics shall be demonstrated by the functional tests. The functional tests corresponding to the assumption family are shown in Table 10-1. The developer may use one or more tests shown in Clauses 7, 8 and 9 in [ISO/IEC 23837-2] for the above purpose. The threshold values (expected values) of these tests in developer's test plan document shall be consistent with the functional specification or the TOE design and with values of realistic characteristics of the assumptions in the security proof.
安全性証明の仮定が現実的な特性の値で記述されている場合、テスト可能なパラメータ/特性の対応する値は機能テストによって実証されなければならない。仮定のファミリに対応する機能テストを Table 10-1 に示す。開発者は、上記の目的のために、[ISO/IEC 23837-2]の 7, 8, 9 章に示されている 1 つ以上のテストを使用してもよい。開発者のテスト計画文書内のこれらのテストのしきい値（期待値）は、機能仕様または TOE 設計、及び、セキュリティ証明の仮定の現実的な特性値と一貫していなければならない。

Table 10-1 Correspondence of assumption families and functional tests

QKD transmitter	
Assumption family	**Phase randomization**
Functional tests	Subsubsection 10.3.2.1, [ISO/IEC 23837-2] 7.7
Testable parameter(s)	The difference between the probability distribution of the measured intensity after passing through an asymmetric Mach-Zehnder interferometer and the theoretical probability distribution 非対称マッハ・ツェンダー干渉計を通った後に測定された強度の確率分布と理論上の確率分布の差 d_{phase}
Assumption family	**Photon statistics and intensity**
Functional tests	Subsubsection 10.3.2.2, [ISO/IEC 23837-2] 7.2
Testable parameter(s)	Deviation between the measured value of k-th order correlation function and the theoretically expected value k 次の相関関数の測定値と理論的に予想される値との偏差 $\Delta^{(k)}$
Assumption family	**Degrees of freedom**
Functional tests	Subsubsection 10.3.2.3, [ISO/IEC 23837-2] 7.6
Testable parameter(s)	The maximum absolute value of the difference in time of arrival, spectrum, azimuthal angle and ellipticity of the polarization between two encoded states 2つのエンコードされた状態間の到着時間、スペクトル、偏光の方位角と楕円率の差の絶対値の最大値 $\delta_{\mathrm{max},t}, \delta_{\mathrm{max},\lambda}, \delta_{\mathrm{max},\theta}, \delta_{\mathrm{max},\varepsilon}$
Assumption family	**Security and cryptographic boundaries**
Functional tests	Subsubsection 10.3.2.4, [ISO/IEC 23837-2] 7.8, 7.9, 7.10
Testable parameter(s)	The minimum value of isolation measured under different conditions (input power and wavelength) in the isolation component being tested テストするアイソレーションコンポーネントにおいて、異なる条件(入力パワーや波長)で測定されたアイソレーションの中の最小値 p_{minIso} The maximum values of injection power for CW light and pulsed light indicating exceptional events 例外イベントを示す CW 光およびパルス光の注入パワーの最大値 $p_{\mathrm{maxCWcont}}, p_{\mathrm{maxPulse}}$ The maximum values of deviations in intensity, spectrum, and phase induced by laser injection

	レーザの注入によって引き起こされる強度、スペクトル、位相のずれの最大値 $d_{\mathrm{maxInt}}, d_{\mathrm{maxSpec}}, d_{\mathrm{maxPhase}}$
Assumption family	**Accuracy of the encoding**
Functional tests	Subsubsection 10.3.2.5, [ISO/IEC 23837-2] 7.5
Testable parameter(s)	The minimum fidelity between the measured density matrix and the ideal density matrix assumed in the QKD protocol 測定された密度行列と QKD プロトコルで仮定される理想的な密度行列とのフィデリティの最小値 F
Assumption family	**Independence of adjacent pulses**
Functional tests	Subsubsection 10.3.2.6, [ISO/IEC 23837-2] 7.4
Testable parameter(s)	Deviation of the average intensity of light pulses prepared with the same intensity setting 同じ強度設定で準備された光パルスの平均強度のずれ $\delta_{k,j,i}$
QKD receiver	
Assumption family	**Detection efficiency**
Functional tests	Subsubsection 10.3.3.1, [ISO/IEC 23837-2] 8.2
Testable parameter(s)	The maximum value of detection probability mismatch between two encoded states 2つのエンコードされた状態間の検出確率不一致の最大値 $\sigma_{\max}$
Assumption family	**Degrees of freedom**
Functional tests	Subsubsection 10.3.3.2, [ISO/IEC 23837-2] 8.2
Testable parameter(s)	The maximum value of detection probability mismatch between two encoded states 2つのエンコードされた状態間の検出確率不一致の最大値 $\sigma_{\max}$
Assumption family	**Security boundary on optical channel**
Functional tests	Subsubsection 10.3.3.3, [ISO/IEC 23837-2] 8.3, 8.4, 8.5
Testable parameter(s)	The maximum value of back-flash probability バックフラッシュ確率の最大値 P_{maxBF} The minimum value of isolation measured under different conditions (input power and wavelength) in the isolation component being tested テストするアイソレーションコンポーネントにおいて、異なる条件(入力パワーや波長)で測定されたアイソレーションの中の最小値 p_{minIso} The maximum values of injection power for CW light and pulsed light indicating exceptional events 例外イベントを示す CW 光およびパルス光の注入パワーの最大値 $p_{\mathrm{maxCWcont}}, p_{\mathrm{maxPulse}}$
Assumption family	**Accuracy of the demodulation**
Functional tests	Subsubsection 10.3.3.4
Testable parameter(s)	The maximum quantum bit error rate in each basis 各基底における量子ビット誤り率の最大値

	$QBER_{\max}$
Assumption family	**Single-photon sensitivity**
Functional tests	Subsubsection 10.3.3.5, [ISO/IEC 23837-2] 8.6
Testable parameter(s)	The ratio of photon detection efficiency with and without blind light Blind 光を入射した場合と入射しない場合の光子検出効率の比 κ
Assumption family	**Recovery or dead time**
Functional tests	Subsubsection10.3.3.6, [ISO/IEC 23837-2] 8.7
Testable parameter(s)	None. Verify that no detection signals are output during dead time. なし。デッドタイム中に検出信号が出力されないことを確認する
Whole of the TOE	
Assumption family	**Calibration**
Functional tests	Subsubsection 10.3.4.1 , [ISO/IEC 23837-2] 9.2
Testable parameter(s)	The maximum value of basis bias and bit bias when a tampering device inserted into a quantum channel causes temporal shifts in the detection efficiency 量子チャネルに挿入される改竄装置によって検出効率に時間的なずれを発生させた時の、基底偏りとビット偏りの最大値 $b_{\max 0}, b_{\max 1}, B_{\max}$
Assumption family	**Stabilities of the light source and the photon detector**
Functional tests	**The light source:** Subsubsection 10.3.4.2 , [ISO/IEC 23837-2] 7.3
	The photon detector: None. The TOE user shall periodically inspect the photon detector for performance degradation. なし。TOE 利用者は、単一光子検出器に性能劣化がないことを定期的に検査する。
Testable parameter(s)	**The light source:** Mean photon number at each intensity 各強度での平均光子数
	The photon detector: None
Assumption family	**Robustness against provoked damage**
Functional tests	Subsubsection 10.3.4.3 , [ISO/IEC 23837-2] 8.9
Testable parameter(s)	The maximum value of the mismatch in detection efficiency of each photon detector after injecting light into the receiver 受信機に光を注入した後の、各単一光子検出器の検出効率のミスマッチの最大値 $\sigma_{\max \mathrm{Mis}}$
Assumption family	**Authenticated classical channel**
Functional tests	Subsection 10.2
Testable parameter(s)	None
Assumption family	**Random number generator**
Functional tests	Subsection 10.6
Testable parameter(s)	None

10.3.2.Assumption families of the QKD transmitter

10.3.2.1. Phase randomization

The test of this assumption family may be conducted according to [ISO/IEC 23837-2] 7.7 EA to test the uniform distribution of the global phase of optical pulses.
When conducting this test, unattenuated light may be used.
この仮定のファミリのテストは、[ISO/IEC 23837-2] 7.7 EA to test the uniform distribution of the global phase of optical pulses に従って実行することができる。
テストの実行においては減衰させない光を用いてもよい。

10.3.2.2. Photon statistics and intensity

The test of this assumption family may be conducted according to [ISO/IEC 23837-2] 7.2 EA to test the photon-number distribution of optical pulses.
この仮定のファミリのテストは、[ISO/IEC 23837-2] 7.2 EA to test the photon-number distribution of optical pulses に従って実行することができる。

10.3.2.3. Degrees of freedom

The test of this assumption family may be conducted according to [ISO/IEC 23837-2] 7.6 EA to test the indistinguishability of encoded states.
When conducting this test, unattenuated light may be used.
この仮定のファミリのテストは、[ISO/IEC 23837-2] 7.6 EA to test the indistinguishability of encoded states に従って実行することができる。
テストの実行においては減衰させない光を用いてもよい。

10.3.2.4. Security and cryptographic boundaries

The test of this assumption family may be conducted according to following tests.

- [ISO/IEC238737-2] 7.8 EA to test the degree of optical isolation of the TX module
  The developer only needs to measure the characteristics of the isolator.
- [ISO/IEC238737-2] 7.9 the sensitivity of the injected light monitor in the TX module
  The developer only needs to measure the characteristics of the light injection monitor.
- [ISO/IEC23837-2] 7.10 the robustness of the TX module against laser injection
  The developer measures that the characteristics of the transmitted light do not change even when light is injected into the QKD transmitter. When conducting this test, unattenuated light may be used.

この仮定のファミリのテストは、以下のテストに従って実行することができる。

- [ISO/IEC238737-2] 7.8 EA to test the degree of optical isolation of the TX module
  開発者はアイソレータの特性を測るだけでよい。
- [ISO/IEC238737-2] 7.9 the sensitivity of the injected light monitor in the TX module
  開発者は光注入モニタの特性を測ればよい。
- [ISO/IEC23837-2] 7.10 the robustness of the TX module against laser injection
  開発者は、QKD 送信機に光の注入をしても送信光の特性が変わらないことを測定する。テストの実行においては減衰させない光を用いてもよい。

10.3.2.5. Accuracy of the encoding

The test of this assumption family may be conducted according to [ISO/IEC 23837-2] 7.5 EA to test the accuracy of state encoding.
When conducting this test, unattenuated light may be used.
この仮定のファミリのテストは、[ISO/IEC 23837-2] 7.5 EA to test the accuracy of state encoding に従って実行することができる。
テストの実行においては減衰させない光を用いてもよい。

Note 1
It is necessary to estimate the density matrices of the photon states at the transmitter output to perform [ISO/IEC 23837-2] 7.5 EA. This application note provides a method for the density matrix estimation.
[ISO/IEC 23837-2] 7.5EA を実行するには送信機の出力における光子状態の密度行列を推定する必要がある．このアプリケーションノートは密度行列推定の一つの方法を与えるものである．
密度行列の求め方は次の通りである。

This method requires transmitting optical pulses with a fixed quantum state from the QKD transmitter. The developer shall provide a function dedicated for this transmission.
　この方法は、送信機から固定の量子状態で光パルスを送信する必要がある。開発者は、この送信専用の機能を提供しなければならない。
This method also requires a reference receiver that outputs correctly for inputs in the correct state.　The receiver measures the states in X-, Y-, and Z- basis. The tester shall prepare such a receiver.
　この方法はまた，正しい入力に対して正しく出力する基準受信機を必要とする．この受信機は X,Y,Z 基底で状態を測定できなければならない．試験者はこのような受信機を準備しなければならない．

Method (state tomography):
方法（状態トモグラフィ）
In the following, the TOE is assumed to use X basis and Z basis to perform the BB84 protocol. The tester selects one of the four states Φ_i $(\Phi \in \{X,Z\}, i = \{0,1\})$ and outputs it from the transmitter.
The transmitted light is measured in the X,Y,Z basis using a reference receiver to obtain the detection rate $P(\Psi_j|\Phi_i), (\Psi \in \{X,Y,Z\}, j = \{0,1\}))$.
　以下では TOE は BB84 プロトコルを実行するために X 基底と Z 基底を用いるものと仮定する。試験者は 4 状態のうちの 1 つΦ_i $(\Phi \in \{X,Z\}, i = \{0,1\})$を選択して送信機から出力する。試験者は光の状態を基準受信機で X,Y,Z 基底で測定し，検出率$P(\Psi_j|\Phi_i), (\Psi \in \{X,Y,Z\}, j = \{0,1\}))$ を得る．
Then, the density matrix on the basis Φ can be calculated. For example, the density matrix on X basis is reconstructed as a linear expansion with Pauli matrices $\hat{\sigma_i}$'s as

$$\rho = \frac{1}{2}\sum_{i=0}^{3} \frac{S_i}{S_0}\hat{\sigma_i},$$

where

$$S_0 = 2n_0$$
$$S_1 = 2(n_1 - n_0)$$
$$S_2 = 2(n_2 - n_0)$$
$$S_3 = 2(n_3 - n_0)$$

$$n_0 = \frac{N}{2}(\langle 0|\rho_{\mathrm{X}}|0\rangle + \langle 1|\rho_{\mathrm{X}}|1\rangle) = P(Z_0|\mathrm{X}_0) + P(Z_0|\mathrm{X}_1) + P(Z_1|X_0) + P(Z_1|X_1)$$

$$n_1 = N\langle 0|\rho_{\mathrm{X}}|0\rangle = P(Z_0|X_0) + P(Z_0|X_1)$$
$$n_2 = N\langle \mathrm{X}_1|\rho_{\mathrm{X}}|X_1\rangle = P(X_1|X_0) + P(X_1|X_1)$$
$$n_3 = N\langle Y_1|\rho_X|Y_1\rangle = P(Y_1|X_0) + P(Y_1|X_1)$$

The accuracy of the encoding is characterized by the fidelity between the intended state and the emitted state.

次に、基底Φ上の密度行列を計算することができる。例えば、X 基底上の密度行列は、次のパウリ行列$\hat{\sigma_i}'$として線形展開として再構成される。

$$\rho = \frac{1}{2}\sum_{i=0}^{3} \frac{S_i}{S_0}\hat{\sigma_i},$$

ここで

$$S_0 = 2n_0$$
$$S_1 = 2(n_1 - n_0)$$
$$S_2 = 2(n_2 - n_0)$$
$$S_3 = 2(n_3 - n_0)$$

$$n_0 = \frac{N}{2}(\langle 0|\rho_{\mathrm{X}}|0\rangle + \langle 1|\rho_{\mathrm{X}}|1\rangle) = P(Z_0|\mathrm{X}_0) + P(Z_0|\mathrm{X}_1) + P(Z_1|X_0) + P(Z_1|X_1)$$

$$n_1 = N\langle 0|\rho_{\mathrm{X}}|0\rangle = P(Z_0|X_0) + P(Z_0|X)$$
$$n_2 = N\langle \mathrm{X}_1|\rho_{\mathrm{X}}|X_1\rangle = P(X_1|X_0) + P(X_1|X_1)$$
$$n_3 = N\langle Y_1|\rho_X|Y_1\rangle = P(Y_1|X_0) + P(Y|X_1)$$

符号化の精度は、意図した状態と出力された状態の忠実度によって特徴付けられる。

References

Daniel F. V. James, *et al*, Physical review A, **64**, 052312 (2001)

Weiyang Zhang, Yu Kadosawa, Akihisa Tomita, Kazuhisa Ogawa, and Atsushi Okamoto, "State preparation robust to modulation signal degradation by use of a dual parallel modulator for high-speed BB84 quantum key distribution systems", Opt. Express **28**, 13965-13977 (2020).

10.3.2.6. Independence of adjacent pulses

The test of this assumption family may be conducted according to [ISO/IEC 23837-2] 7.4 EA to test the independence of the intensities of optical pulses.

When conducting this test, unattenuated light may be used.

この仮定のファミリのテストは、[ISO/IEC 23837-2] 7.4 EA to test the independence of the intensities of optical pulses に従って実行することができる。

テストの実行においては減衰させない光を用いてもよい。

10.3.3.Assumption families of the QKD receiver

10.3.3.1. Detection efficiency

The test of this assumption family may be conducted according to [ISO/IEC 23837-2] 8.2 EA to test the consistency of detection probability in the RX module.

When conducting this test, the developer also measures wavelength dependency and time dependency.

この仮定のファミリのテストは、[ISO/IEC 23837-2] 8.2 EA to test the consistency of detection probability in the RX module に従って実行することができる。
テストの実行においては、開発者は波長依存性と時間依存性も測定する。

10.3.3.2. Degrees of freedom

The test of this assumption family may be conducted according to [ISO/IEC 23837-2] 8.2 EA to test the consistency of detection probability in the RX module. In addition, the developer conducts the functional test described in Subsubsection10.9.2.2. However, it is not necessary to carry out each test separately, and it is acceptable to standardize them as long as the same information can be obtained.
この仮定のファミリのテストは、[ISO/IEC 23837-2] 8.2 EA to test the consistency of detection probability in the RX module に従って実行することができる。加えて 10.9.2.2 に記載されている機能テストも実施する。ただしそれぞれのテストを別々に実施する必要はなく、同じ情報が得られる限り共通化してもよい。

10.3.3.3. Security boundary on optical channel

The test of this assumption family may be conducted according to following tests.
この仮定のファミリのテストは次のテストに従って実施してよい。

- [ISO/IEC 23837-2] 8.3 EA to test information leakage of back-flashes from the RX module
- [ISO/IEC 23837-2] 8.4 EA to test the degree of optical isolation of the RX module
- [ISO/IEC 23837-2] 8.5 EA to test the sensitivity of the injected light monitor in the RX module

10.3.3.4. Accuracy of the demodulation

This test demonstrates the accuracy of the demodulation in the receiver.
このテストでは受信機における復調の精度を実証する。
Input the signal transmitted from a transmitter that has passed functional testing 10.3.2.5. (Accuracy of the encoding) or its replacement into the receiver under test. From the measurement results of the receiver, calculate the quantum bit error rates $QBER_X$ and $QBER_Z$ for each basis. The larger of the two is designated as $QBER_{max}$.
10.3.2.5. (Accuracy of the encoding) の機能テストに合格した送信機もしくはその代替品から送信された信号をテスト対象の受信機に入力する。受信機での測定結果から、各基底における量子ビット誤り率 $QBER_X, QBER_Z$ を算出する。このうち大きい方を $QBER_{max}$ とする。

10.3.3.5. Single-photon sensitivity

The test of this assumption family may be conducted according to [ISO/IEC 23837-2] 8.6 EA to test the robustness of the RX module against bright light blinding. In addition, the developer conducts the functional test described in Subsubsection 10.9.2.1. However, it is not necessary to carry out each test separately, and it is acceptable to standardize them as long as the same information can be obtained.
この仮定のファミリのテストは、[ISO/IEC 23837-2] 8.6 EA to test the robustness of the RX module against bright light blinding に従って実行することができる。加えて 10.9.2.1 に記載されている機能テストも実施する。ただしそれぞれのテストを別々に実施する必要はなく、同じ情報が得られる限り共通化してもよい。

10.3.3.6. Recovery or dead time

The test of this assumption family may be conducted according to [ISO/IEC 23837-2] 8.7 EA to test the

appropriateness of dead time settings of SPDs.
この仮定のファミリのテストは、[ISO/IEC 23837-2] 8.7 EA to test the appropriateness of dead time settings of SPDs に従って実行することができる。

10.3.4.Assumption families of the whole of the TOE

10.3.4.1. Calibration

The test of this assumption family may be conducted according to [ISO/IEC 23837-2] 9.2 EA to test the inducibility of detection probability mismatch.
この仮定のファミリのテストは、[ISO/IEC 23837-2] 9.2 EA to test the inducibility of detection probability mismatch に従って実行することができる。

10.3.4.2. Stabilities of the light source and the photon detector

The light source

The test of the light source of this assumption family may be conducted according to [ISO/IEC 23837-2] 7.3 EA to test the mean photon number and stability of optical pulses.
When conducting this test, unattenuated light may be used.
この仮定のファミリの光源のテストは、[ISO/IEC 23837-2] 7.3 EA to test the mean photon number and stability of optical pulses に従って実行することができる。
テストの実行においては減衰させない光を用いてもよい。

The photon detector

There are no tests for the photon detector for this assumption family. The TOE user shall periodically inspect the photon detector to ensure that there is no deterioration in their performance to guarantee their stability.
この仮定のファミリの単一光子検出器についてのテストはない。TOE 利用者は単一光子検出器の安定性を保証するため、単一光子検出器に性能劣化がないこと定期的に検査する。

10.3.4.3. Robustness against provoked damage

This assumption family does not require functional tests. The developer shall provide the guidance document for consumers to regularly maintain and inspect the QKD receiver and the QKD transmitter. Contents of the guidance are evaluated for appropriateness by the work units shown in section 3.2.
この仮定のファミリには機能テストを必要としない。開発者は、消費者向けに定期的に QKD 受信機、QKD 送信機を保守点検するよう、ガイダンスを提供しなければならない。ガイダンスの内容は、3.2 節に示されるワークユニットによって適切かどうか評価される。

10.3.5.Functional tests for assumptions other than assumption families

Characteristics that are not subject of tests of assumption families described above, but that corresponds to the assumptions in the security proof, shall be also demonstrated by the functional testes. The developer may use one or more tests shown in Clause 7, 8 and 9 in [ISO/IEC 23837-2] for the above purpose. The threshold value (expected value) of these tests in developer's test plan document shall be consistent with the functional specification or the TOE design.
上記に述べられている仮定のファミリのテスト対象ではない、セキュリティ証明の仮定に対応する特性も、機能

テストによって実証されなければならない。開発者は、上記の目的のために、[ISO/IEC 23837-2]の 7, 8, 9 章に示されている 1 つ以上のテストを使用してもよい。開発者のテスト計画文書内のこれらのテストのしきい値（期待値）は、機能仕様または TOE 設計と一貫していなければならない。

10.4. FPT_PHP.3

This test demonstrates the behaviour of the light injection monitor (FPT_PHP.3).
このテストは FPT_PHP.3 の機能性である光注入モニタのふるまいを実証する。
If a light injection monitor or filter is implemented for these SFRs, its actual characteristics shall be demonstrated by the functional test. If the light injection monitor is implemented, the test demonstrates power of injected light detected by the light injection monitor. If the sensitivity of the monitor changes with parameters such as wavelength, the sensitivity shall be demonstrated by changing the parameters. And more, the test demonstrates that the TSF automatically responds to monitor detection consistent with its functional specification. If the filter is implemented, such as a wavelength filter, the test demonstrates attenuation characteristics of the filter. In this case, filtering out itself is automatic responses of the TSF, so no additional testing that demonstrates automatic response is required. The developer may use one or more tests shown in Clause 7, 8 and 9 in [ISO/IEC 23837-2] for the above purpose. The threshold value (expected value) of these tests in developer's test plan document shall be consistent with the functional specification or the TOE design.
これらの SFR の為に光注入モニタやフィルタが実装されている場合、機能テストによってその特性を実証しなければならない。光注入モニタが実装されているならば、テストは、光注入モニタによって検出される注入光の強さを実証する。モニタの感度が波長などのパラメータによって変化する場合は、パラメータを変化させて感度を実証する。更に、テストは、モニタの検出に対して、TSF が機能仕様と一貫した自動応答をする事を実証する。波長フィルタのようなフィルタが実装されているならば、テストは、フィルタの減衰特性を実証する。この場合、フィルタによる除去自身が TSF の自動応答であるため、自動応答を実証する追加のテストは必要ない。開発者は、上記の目的のために、[ISO/IEC 23837-2]の 7, 8, 9 章に示されている 1 つ以上のテストを使用してもよい。開発者のテスト計画文書内のこれらのテストのしきい値（期待値）は、機能仕様または TOE 設計と一貫していなければならない。

10.5. FPT_FLS.1

This SFR requires that a secure state is preserved when some types of failures occur. In [PP-EAL4] case, state control is also required, but in [PP-EAL2] case, no state control is required. The common test scenario may be as follows, but if the TOE claims [PP-EAL4] compliant, the test scenario should be more refined in the developer's test plan document in order to demonstrate the state control.
この SFR は、いくつかのタイプの障害が発生したときに安全な状態の維持を要求する。[PP-EAL4]の場合はステート制御も要求されるが、[PP-EAL2]の場合はステート制御を要求されない。共通のテストシナリオは次の通りであるが、TOE が[PP-EAL4]準拠を主張する場合、ステート制御を実証するために、テストシナリオはさらに開発者のテスト計画書文書で詳細化されるべきである。

Test 1:
This test demonstrates the FPT_FLS.1 functionality of maintaining the secure state when the failures occur.
このテストは FPT_FLS.1 の機能性である障害発生時のセキュア状態の維持を実証する。
Step 1. The tester shall reproduce the situation in which each failure occurs.

試験者は、各障害が発生した状況を再現しなければならない。

Step 2. The tester shall verify that the defined secure state in each PP is preserved.

試験者は、各 PP で定義された安全な状態が維持されたことを確認しなければならない。

It is expected that the developer shall provide test tools (e.g. debugger) or dedicated test interfaces that can access TSF data in order to reproduce the failure situation such as authentication failure of the classical channel. Depending on assignment of self-test SFR, the failure situation cannot be reproduced even if test tools or test interfaces are provided. For example, it is so difficult to reproduce the failure of the physical random number generator. It is acceptable to exclude such failures from this test. Assurance for such self-test function and secure state preservation function are provided only by document examination.

開発者は、障害状況（古典チャネルの認証失敗など）を再現するために、TSF データにアクセスできるテストツール（デバッガなど）または専用のテストインターフェースを提供しなければならないと予想される。自己テスト SFR の割付けによっては、テストツールやテストインターフェースが提供されても、障害の状況を再現することはできない。例えば、物理乱数生成器の障害を再現することは非常に困難である。このような障害をこのテストから除外することは許容される。このような自己テスト機能と安全な状態維持機能の保証は、文書検査によってのみ提供される。

10.6. FCS_RNG.1

The developer shall test the random number generator according to the random number generator standard associated with the SFR. For example, the standard may be AIS31 or SP800-90B.

開発者は、乱数生成器を SFR に関連付けられた乱数生成器標準に従ってテストしなければならない。例えば、標準は AIS31 または SP800-90B であり得る。

10.7. FCS_COP.1 and FCS_CKM.6

Depending on certification scheme, specific algorithm verification program may be required for crypto algorithms specified in FCS component. The developer should contact each certification body for the required algorithm testing.

認証スキームに依存して、FCS コンポーネントで指定された暗号アルゴリズムには、特定のアルゴリズム検証プログラムが要求される場合がある。開発者は、要求されるアルゴリズムテストについて、それぞれの認証機関に問い合わせるべきである。

The test for the destruction of the cryptographic keys specified in FCS_CKM.6 can be tested with reference to the supporting documents [DSCSD] or [HCDSD].

FCS_CKM. 6 で指定された暗号鍵の破棄のテストは、サポート文書[DSCSD], [HCDSD]を参考にしてテストすることができる。

10.8. Other SFR in the Functional Package

Functional tests of the identification and authentication specified in FIA_UIA_EXT.1 and the secure channel protocol specified in FTP_ITC.1 shall be tested with reference to the supporting document [NDSD].

The use of trusted channels specified in FDP_ETC_EXT.2.1 is included in the tests for FTP_ITC.1.

FIA_UIA_EXT.1 で指定された識別認証の機能テストと、FTP_ITC.1 で指定されたセキュアチャネルプロトコル

の機能テストはサポート文書[NDSD]を参考にしてテストする。
FDP_ETC_EXT.2.1 で指定された信頼されたチャネルの使用は、FTP_ITC.1 のテストに含まれる。

Test 1:

This test demonstrates the FDP_ETC_EXT.2 functionality that is exporting QKD keys and that the exported keys are not re-used.
このテストは FDP_ETC_EXT.2 の機能性である QKD 鍵のエクスポートとエクスポートした鍵が再利用されないことを実証する。

Step 1. The tester shall start QKD session.
試験者は QKD セッションを開始しなければならない。

Step 2. The tester shall ensure that the TOE automatically exports the QKD key to the key manager during the QKD session. The export shall be done only once and it shall be ensured that the exported QKD keys are not re-used.
試験者は、QKD セッション中に TOE が鍵マネージャに QKD 鍵を自動的にエクスポートすることを確認しなければならない。エクスポートは一度のみであり、エクスポートした QKD 鍵が再利用されないことを確認しなければならない。

10.9. Functional tests related with vulnerability analysis

10.9.1.QKD transmitter

At the moment, functional tests related with vulnerability analysis on the QKD transmitter have not been identified yet.
現在、QKD 送信機の脆弱性分析に関連する機能テストは、まだ特定されていない。

10.9.2.QKD receiver

10.9.2.1. Single-photon sensitivity

Purpose of test

The test of this assumption family demonstrates the countermeasure against the bright illumination attack.
この仮定のファミリのテストは明光攻撃の対抗策を実証する。

Target of test

A set of receivers used for the TOE.
TOE に使用されている受信機 1 セット。

Test equipment and configuration

- QKD transmitter QKD 送信機
  TOE QKD transmitter or its replacement.
  TOE の送信器あるいはその代替品。
- Fiber spool ファイバスプール
  Fiber spool for the distance envisaged, e.g. 50 km
  50km など、想定する距離のボビンファイバ
- Optical coupler 光カプラ
  For 1550nm

1550nm 用

- Laser for blinding　Blind 用レーザ
  Light source capable of outputting pulsed and CW light in the 600-2000 nm range.
  パルス光、CW 光を 600-2000nm の範囲で出力できる光源

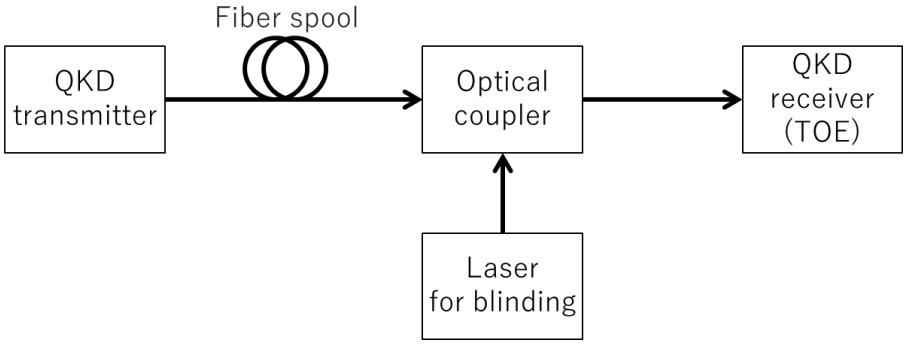

Figure 10-1 Test for bright illumination attack

Test method

Step 1.　Establish a QKD link.
QKD リンクを確立する。

Step 2.　Record the difference $R_i(0)$ between the photon detection rate when no Blind light is input to the receiver and the photon detection rate when the signal light from the transmitter is input to the receiver. i indicates the index of the multiple implemented photon detectors, typically $i = 0,1$ or $i = 0,1,2,3$. The photon detection rate refers to the number of photons detected per unit of time. The input signal light shall be of the intensity and state used in normal key generation.
Blind 光を入力しない状態で、送信機からの信号光を受信機に入力している場合の光子検出レートと信号光を入力しない場合の光子検出レートの差分$R_i(0)$を記録する。iは複数実装されている単一光子検出器のインデックスを示し、典型的には $i = 0,1$ もしくは $i = 0,1,2,3$ である。ここで光子検出レートとは、1 ラウンド当たりの光子検出確率を意味する。光子検出レートの算出には、ブランキング処理により無効化されたラウンドは使用しない。入力する信号光は、通常の鍵生成時に使用する強度や状態とする。

Step 3.　The Blind light source is set to CW (continuous light) mode. Set the Blind light intensity and wavelength to minimum values according to Table 10-2. The intensity is gradually increased and the difference R_i between the photon detection rate with signal light input and without signal light input at each intensity is recorded. The upper limit of the Blind light intensity shall be limited to the maximum value that is not detected by the light injection monitor implemented inside the QKD receiver.
Blind 光源を CW（連続光）モードとする。Table 10-2 に従い Blind 光の強度と波長を最小値に設定する。強度を徐々に増加させ、各強度で信号光を入力している場合の光子検出レートと信号光を入力しない場合の光子検出レートの差分R_iを記録する。Blind 光の強度の上限は、QKD 受信機内部に実装されている光注入モニタで検知されない最大値までとする。

Step 4.　Gradually increase the wavelength and repeat step 3.
波長を徐々に増加させ、ステップ 3 を繰り返し実行する。

Step 5.　The Blind light source is set to pulse oscillation mode. Set the Blind light intensity, wavelength, repetition frequency, pulse width and pulse incidence timing to minimum values according to Table 10-2. The intensity is gradually increased and the difference R_i between the photon detection rate with signal light input and without signal light input at each intensity is recorded.

Blind 光源をパルス発振モードとする。Table 10-2 に従い Blind 光の強度、波長、繰り返し周波数、パルス幅、パルス入射タイミングを最小値に設定する。強度を徐々に増加させ、各強度で信号光を入力している場合の光子検出レートと信号光を入力しない場合の光子検出レートの差分R_iを記録する。

Step 6. Gradually increase the wavelength and repeat step 5.
波長を徐々に増加させ、ステップ 5 を繰り返し実行する。

Step 7. Gradually increase the repetition frequency and repeat steps 5 and 6.
繰り返し周波数を徐々に増加させ、ステップ 5, 6 を繰り返し実行する。

Step 8. Gradually increase the pulse width and repeat steps 5~7.
パルス幅を徐々に増加させ、ステップ 5~7 を繰り返し実行する。

Step 9. Gradually increase the pulse injection timing and repeat steps 5-8.
パルス入射タイミングを徐々に増加させ、ステップ 5~8 を繰り返し実行する。

Step 10. Repeat 1-9 in all modes permitted by the administrator.
1～9 を管理者によって許可されている全てのモードで繰り返す。
The various parameters to be varied in steps 6-9 do not necessarily have to be varied in this order and the order may be interchanged.
なお、ステップ 6~9 で変化させる各種パラメータは必ずしもこの順序で変化させる必要はなく、順序を入れ替えても良い。

Table 10-2 Parameter of blind light

Items	Description
Wavelength	
Minimum	600nm
Maximum	2000nm
Step	10nm
Notes	Evaluation of the transmission characteristics of the QKD receiver (e.g. filters) in advance, for wavelengths with losses <30 dB. 事前に受信機の透過特性（フィルタなど）を評価し、損失<30dB の波長について評価
Pulse width	
Minimum	1/10th of the inverse of the APD bandwidth. Ex: 0.1ns APD 帯域の逆数の 1/10. Ex: 0.1ns
Maximum	Up to the reciprocal of the clock frequency Ex: 0.5ns クロック周波数の逆数まで Ex: 0.5ns
Step	At least 3 points per digit (e.g. 1, 2, 5 times). 1 桁あたり 3 点以上(1,2,5 倍など)
Notes	・"Up to the reciprocal of the clock frequency" is not a problem. ・「クロック周波数の逆数まで」で問題ない
Repetition frequency	

Minimum	--
Maximum	Clock frequency (Ex. 1GHz)
Step	--
Notes	--
Intensity	
Minimum	Minimum pulse energy of received light assumed by the device (distance dependent) Ex: 0.5 Photon/pulse -10dB(Assume 50 km) =0.05 Photon/pulse = 6.4e-21[J]/pulse 装置が想定する受信光のパルスエネルギーの最小値（距離依存） Ex: 0.5 光子/パルス -10dB(50km 想定) =0.05 光子/パルス= 6.4e-21[J]/パルス
Maximum	Up to the light injection monitor detection threshold (see also Notes).or Until they are failed. 光注入モニタ検知閾値まで(Notes 欄も参照) or 不合格になるまで
Step	At least 3 points per digit (e.g. 1, 2, 5 times). 1 桁あたり 3 点以上(1,2,5 倍など)
Notes	If the light injection monitor bandwidth is wide, the clock frequency is taken into account and evaluated up to the effective light injection monitor detection threshold. 光注入モニタ帯域が広い場合はクロック周波数を考慮して、実効的な光注入モニタ検知閾値までを評価する
Timing of incident	
Minimum	0ns（basis）
Maximum	clock cycle Ex: 1ns
Step	1/10th of a clock Ex: 0.1ns
Notes	--

Acceptance criteria

Indicator:

指標：

κ :The ratio of R_i to $R_i(0)$

$R_i(0)$に対するR_iの比 κ

$\kappa = R_i \,/\, R_i(0)$

For κ calculated from all R_i obtained in steps 3~10, $0.95 < \kappa < 1.05$

ステップ 3~10 で得られる全てのR_iから算出される κ について $0.95 < \kappa < 1.05$

10.9.2.2. Degrees of freedom

Purpose of test

The test of this assumption family demonstrates the countermeasure against the time shift attack.

この仮定ファミリのテストはタイムシフト攻撃の対抗策を実証する。

Target of test

A set of receivers used for TOE

TOE に使用されている受信機 1 セット

Test equipment and configuration

- QKD transmitter

  TOE QKD transmitter or its replacement. TOE の QKD 送信機またはその代替品。

  The configuration for this test is shown in Figure 10-2.

  このテストの構成は Figure 10-2 に示す。

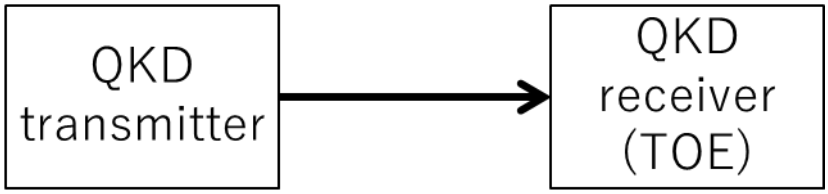

Figure 10-2 Test for time shift attack

Test method

Step 1. Establish a QKD link.

QKD リンクを確立する。

Step 2. Record the photon detection rates, denoted as $R_{\mathrm{X0}}(t), R_{\mathrm{X1}}(t), R_{\mathrm{Z0}}(t)$, and $R_{\mathrm{Z1}}(t)$, for each basis (X, Z) and each bit value (0, 1) while varying the timing t of the gate pulse in the receiver or the incidence timing of the signal light. Here, the photon detection rate refers to the probability of photon detection per round. Both dark counts and photon detections are included in the photon detection rates without distinction.

受信機におけるゲートパルスの印加タイミングもしくは信号光の入射タイミング t を変えながら各基底（X, Z)、各ビット値（0, 1）の光子検出レートを記録し、それぞれ $R_{\mathrm{X0}}(t), R_{\mathrm{X1}}(t), R_{\mathrm{Z0}}(t), R_{\mathrm{Z1}}(t)$ とする。ここで光子検出レートとは、1 ラウンド当たりの光子検出確率を意味する。この時ダークカウントと光子検出は区別せず、両方の検出イベントを光子検出レートに含める。

Step 3. Calculate the ratio $r_{\mathrm{X}}(t), r_{\mathrm{Z}}(t)$ of the two photon detection rates in the same basis at each timing t.

各タイミング t で、同一基底の 2 つの光子検出レートの比 $r_{\mathrm{X}}(t), r_{\mathrm{Z}}(t)$ を計算する。

$$r_{\mathrm{X}}(t) = \frac{R_{\mathrm{X1}}(t)}{R_{\mathrm{X0}}(t)}$$

$$r_{\mathrm{Z}}(t) = \frac{R_{\mathrm{Z1}}(t)}{R_{\mathrm{Z0}}(t)}$$

Step 4. Let the maximum and minimum values obtained from the two bases and all timings t above be r_{max} and r_{min}, respectively

2 つの基底および全てのタイミング t から得られる上記の値のうち、その最大値と最小値をそれぞれ r_{max}, r_{min} とする。

Table 10-3 Parameters of the time shift attack

Items	Description
Gate timing	
Minimum	0ps (basis)
Maximum	Clock frequency Ex. 800ps
Step	Below 1/10 of clock frequency Ex. 25ps
Notes	Evaluate the satellites (and possibly have them pick up the satellites). サテライトも評価する（サテライトを拾わせる可能性もあるので）
Intensity	
Minimum	0
Maximum	Strength at normal operation or just before Bob side strength light injection monitor 通常運用時の強度 or Bob 側強度光注入モニタにかかる直前
Step	None (only the above two) なし。（上記二つのみ）
Notes	The evaluation of the minimum is based on the smallest difference in dark counts. 最小での評価は、ダークカウントの差異が小さいことを評価している。

Acceptance criteria

Pass at $r_{max} < 1.2$ and $r_{min} > 0.8$.

$r_{max} < 1.2$ かつ $r_{min} > 0.8$ であれば合格とする。

11. Penetration Tests

This section outlines penetration tests to exploit vulnerabilities in the TOE for the assumption families. These penetration tests are derived from attacks which have been known in literature.
このセクションでは、仮定のファミリに対して TOE の脆弱性を悪用するための侵入テストの概要を説明する。これらの侵入テストは、文献で既知の攻撃手法を基に作成されている。

11.1. QKD transmitter

11.1.1.Exploitation of imperfect phase randomization

Test 1: Source attacks with phase information

This test requires an auxiliary laser source that emits pulses in the same mode as the pulses from the QKD transmitter.
This test composed of the following two phases:
このテストには、QKD 送信機からのパルスと同じモードでパルスを発する補助レーザ光源が必要である。
このテストは、以下の 2 つのフェーズで構成されている。

Phase 1: Using a train of pulses emitted from the QKD transmitter, the tester adjusts the phase of the auxiliary laser source via injection locking or a feedback loop with a relative phase measurement.
フェーズ 1：QKD 送信機から発せられたパルス列を使用して、試験者は、相対位相測定による注入同期またはフィードバックループを介して補助レーザ光源の位相を調整する。

Phase 2: Using the auxiliary laser source, the tester carries out attacks on the rest of the pulses from the QKD transmitter as described in the References.
フェーズ 2：補助レーザ光源を使用して、参考文献に記載されているように、試験者は QKD 送信機からの残りのパルスに対する攻撃を実施する。

After Phase 1, the tester should verify whether any correlations are made between the phases of the pulses from the QKD transmitter and those from the auxiliary laser source. If no correlations are observed, the test result is PASS with no need for proceeding to Phase 2.
フェーズ 1 の後、試験者は、QKD 送信機からのパルスと補助レーザ光源からのパルスの各フェーズ間に相関関係があるかどうかを確認すべきである。相関関係が観察されなければ、フェーズ 2 に進む必要はなく、テスト結果は合格となる。

References:

H. -K. Lo and J. Preskill, “Phase randomization improves the security of quantum key distribution”, arXiv:quant-ph/0504209.
H. -K. Lo and J. Preskill, “Security of quantum key distribution using weak coherent states with nonrandom phases”, Quant. Inf. Comput. **8** 431-458 (2007).
Y. -L. Tang *et al*., “S Source attack of decoy-state quantum key distribution using phase information”, Phys. Rev. A **88**, 022308 (2013).

11.1.2.Exploitation of degrees of freedom not intentionally used

Test 1: Intercept-resend attack with side information

(*Tentative*)

The following procedure is used when the TOE uses time-bin encoding and the pulses from the QKD transmitter nominally have V polarization.

Step 1. The tester shall place a polarization filter that only passes H polarization followed by a wave plate to change the polarization to V.

Step 2. The tester shall distinguish the bit value in the Z-basis state through photon detection using the same apparatus as the QKD receiver.

Step 3. When the detection has been successful. the tester shall prepare a weak laser pulse in the Z-basis with the observed bit value and send it to the QKD receiver. The tester shall record the observed bit value. When the detection has failed, the tester shall send no light to the QKD receiver.

TOE がタイムビン符号化を使用しており、QKD 送信機からのパルスが通常 V 偏光である場合、以下の手順が使用される。

Step 1. 試験者は、H 偏光のみを通す偏光フィルタを配置し、その後に波長板を配置して偏光を V 偏光に変える。

Step 2. 試験者は、QKD 受信機と同じ装置を使用して光子検出を行い、Z 基底状態のビット値を識別する。

Step 3. 検出が成功した場合、テスターは観測されたビット値で Z 基底状態の弱いレーザパルスを準備し、それを QKD 受信機に送信する。試験者はビット値を記録しなければならない。検出が失敗した場合、試験者は光を送信せず、QKD 受信機に何も送らない。

Acceptance criteria

The tester shall use the criteria described in Subsection 11.4.

試験者は 11.4 節に記載されているクライテリアを使用しなければならない。

Test 2: Side-channel filtering attack:

(*Tentative*)

The following procedure is used when the TOE uses time-bin encoding.

Step 1. The tester shall prepare a transmission filter (for polarization/temporal modes/spectral modes) that has different transmissivities for the two Z-basis states with bit values 0 and 1.

Step 2. The tester shall insert the filter in the quantum channel between the QKD transmitter and the QKD receiver.

Step 3. The tester shall record the bit value with the higher transmissivity.

TOE が時間ビン符号化を使用する場合、以下の手順が用いられる。

Step 1. 試験者は、ビット値 0 と 1 の 2 つの Z 基底状態に対して異なる透過率を持つ伝送フィルタ（偏波/時間モード/スペクトルモード用）を用意する。

Step 2. 試験者は、QKD 送信機と QKD 受信機間の量子チャネルにフィルタを挿入する。

Step 3. 試験者は、より高い透過率のビット値を記録する。

Acceptance criteria

The tester shall use the criteria described in Subsection 11.4.

試験者は 11.4 節に記載されているクライテリアを使用しなければならない。

11.1.3.Exploitation of invalid security and cryptographic boundaries

Test 1: Trojan horse attack

The following procedure is used when the TOE decoy-state BB84 protocol generates sifted keys from the Z-basis only and the X-basis is only used to monitor eavesdropping.

TOE の decoy-state BB84 プロトコルが Z 基底のみからシフト鍵を生成し、X 基底が盗聴の監視のみに使用される場合、以下の手順が使用される。

Step 1. The tester prepares a light source (probe light source, henceforth) for probing the internal state of the QKD transmitter to learn its choices of the basis and the bit value.

試験者は、QKD 送信機の内部状態をプローブして、その基底の選択とビット値を把握するための光源（以下プローブ光源）を用意する。

Step 2. For each of the M rounds comprising a QKD session, the tester shall inject light from the probe light source to the QKD transmitter and make a measurement on the reflected light to obtain an outcome (probe outcome, henceforth). Then, depending on the outcome, the tester shall choose one from the following options. (Some options may not be available for a high-speed TOE).

QKD セッションを構成する M ラウンドのそれぞれについて、試験者はプローブ光源から QKD 送信機に光を注入し、反射光を測定して結果（プローブ結果）を取得しなければならない。次に、結果に応じて、試験者は以下のオプションから 1 つを選択する。(高速 TOE では、一部のオプションが利用できない場合がある)。

i) Block the encoded pulse(s) the QKD transmitter sends out for the round and send a brighter encoded pulse(s) instead to the QKD receiver.

Note that this option is effective if, from the probe outcome, it is highly probable that the QKD transmitter chose the Z-basis and the encoded bit value can be guessed with high confidence.

i) QKD 送信機がそのラウンドで送信する符号化パルスをブロックし、代わりに QKD 受信機に明るい符号化パルスを送信する。

このオプションは、プローブの結果から、QKD 送信機が Z 基底を選択した可能性が高く、符号化されたビット値を高い信頼性で推測できる場合に有効であることに注意すること。

ii) Measure the encoded pulse(s) the QKD transmitter sends out for the round on the Z basis. If the bit value was successfully determined, send the corresponding bright encoded pulse on the Z-basis to the QKD receiver. Otherwise, sends no light to the QKD receiver.

Note that this option is effective if, from the probe outcome, it is highly probable that the QKD transmitter chose the Z-basis.

ii) QKD 送信機がそのラウンドで送出する符号化パルスを Z 基底で測定する。ビット値が正常に決定された場合、対応する明るい符号化パルスを Z 基底で QKD 受信機に送信する。そうでない場合は、QKD 受信機に光を送信しない。

このオプションは、プローブの結果から、QKD 送信機が Z 基底を選択した可能性が高い場合に有効であることに注意すること。

iii) Let the encoded pulse(s) from the QKD transmitter pass through for the round.

Note that choosing this option over the next option is effective if the encoded bit value can be guessed with high confidence from the probe outcome.

Iii) QKD 送信機からの符号化パルスをラウンドの間通過させる。
このオプションを次のオプションよりも優先させるのは、プローブの結果から暗号化されたビット値を高い確度で推測できる場合に有効であることに注意すること。

iv) Block the encoded pulse(s) the QKD transmitter sends out for the round and sends no light to the QKD receiver.
QKD 送信機がそのラウンドで送信する符号化パルスをブロックし、QKD 受信機には光を送信しない。

Step 3. After following the procedure described in one of the above options, the tester shall determine a bit value which is more likely and record it.
試験者は上記のオプションのひとつを実施した後、可能性が高いビット値を決定し記録する。

Acceptance criteria

The tester shall use the criteria described in Subsection 11.4.
試験者は 11.4 節に記載されているクライテリアを使用しなければならない。

11.1.4.Exploitation of inaccuracy in encoding

Test 1: Intercept-resend attack on the monitoring basis

(*Tentative*)

The following procedure is used when the TOE decoy state BB84 protocol generates sifted keys from the Z-basis only and the X-basis is only used to monitor eavesdropping.
TOE decoy-state BB84 プロトコルが Z 基底のみから選択された鍵を生成し、X 基底が傍受の監視のみに使用される場合、以下の手順が使用される。

The tester shall in advance determine the states of the optical pulse(s) emitted from the QKD transmitter for the bit values 0 and 1 in the X-basis. The tester shall then construct the averaged density operator of a single photon in the encoded degree of freedom to determine the two orthogonal modes that diagonalize the operator. The basis formed by the two modes is called X'-basis henceforth.
試験者は、X 基底におけるビット値 0 と 1 について、QKD 送信機から放出される光パルスの状態を事前に決定する。次に、試験者は、符号化された自由度における単一光子の平均密度演算子を構築し、その演算子を対角化する 2 つの直交モードを決定する。このモードからなる基底は、以降 X'基底と呼ばれる。

The tester shall choose the rate t at which the attack is conducted. During a QKD session consisting of M rounds, the tester shall select Mt rounds and carry out the following attacks for each round.

Step 1. The tester shall measure the pulse(s) from the QKD transmitter on the X'-basis to distinguish the two orthogonal modes.

Step 2. If the measurement at Step 1 has succeeded in the distinction, the tester shall prepare a bright pulse in the corresponding mode and send it to the QKD receiver. If a sifted key bit was produced in the round, the tester shall guess the bit value from the measurement outcome and record it.

Step 3. If the measurement at Step 1 has failed, the tester sends the vacuum to the QKD receiver.

攻撃者は、攻撃を実施する比率 t を選択する。Mラウンドで構成される QKD セッション中、攻撃者はMtラウンドを選択し、各ラウンドに対して以下の攻撃を実施する。

ステップ 1. 試験者は、二つの直交モードを区別するため X'基底で QKD 送信機からのパルスを測定する。
ステップ 2. ステップ 1 の測定で区別が成功した場合、試験者は対応するモードで明るいパルスを準備し、それを QKD 受信機に送信する。ラウンドでシフト鍵ビットが生成された場合、試験者は測定結果からビット値を推測し、それを記録する。
ステップ 3. ステップ 1 の測定に失敗した場合、試験者は QKD 受信機に真空状態を送信する。

Acceptance criteria

The tester shall use the criteria described in Subsection 11.4.
試験者は 11.4 節に記載されているクライテリアを使用しなければならない。

11.2. QKD receiver

11.2.1.Exploitation of detection efficiency mismatch for different degrees of freedom

Test: {time, polarization, wavelength} shift attack

Target of test

A set of the QKD transmitter and the QKD receiver that used in TOE
TOE に使用されている QKD 送信機と受信機の 1 セット

Test equipment and configuration

- QKD transmitter (TOE)
- QKD receiver (TOE)
-Shifting device; Timing controller for time shift attack, Polarization controller for polarization shift attack, Wavelength controller for wavelength shift attack

－QKD 送信機（TOE）
－QKD 受信機（TOE）
－シフティングデバイス：タイムシフト攻撃用のタイミングコントローラ、偏光シフト用の偏光コントローラ、波長シフト攻撃用の波長コントローラ

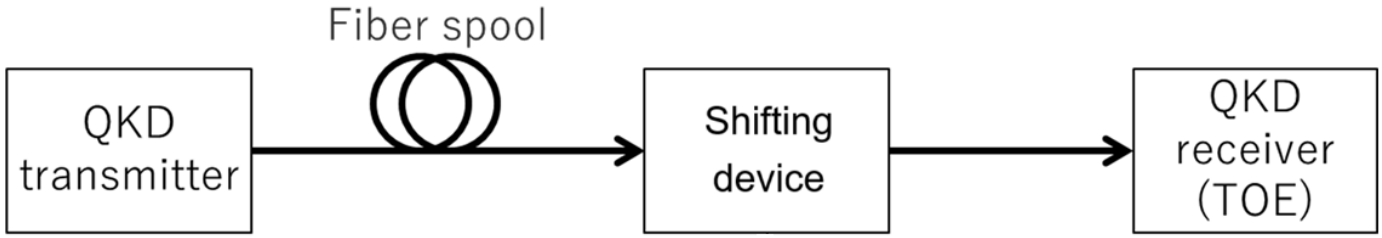

Figure 11-1 Test configuration for {time, polarization, wavelength} shift attack

Test method

The tester chooses a degree of freedom from time, polarization, and wavelength for attack, and inserts the shifting device for the degree of freedom on the optical channel between the transmitter and the receiver.
Step 1. The tester shifts the degree of freedom with an amount of shift.
Step 2. The tester sends bit strings from the transmitter and records the detection events.
Step 3. The tester set the bit value to a fixed value (0 or 1) for the detection events.

Repeat Step 2 and Step 3 for M rounds.

The tester changes the amount of shift and continues step 2 and step 3.

試験者は攻撃のため時間、偏光、波長のうち自由度を選択し、送信機と受信機の間の光チャネルへ自由度用のシフティングデバイスを挿入する。

Step 1.　試験者はシフト量をもって自由度をシフトする。

Step 2.　試験者は送信機からビット列を送信し、検知デバイスで記録する。

Step 3.　試験者は検知イベントに対しビット値を固定値（0 あるいは 1）にセットする。

Step 2 と 3 を M ラウンド繰り返す。

試験者はシフト量を変更し Step 2 と 3 を続ける。

Acceptance criteria

The tester shall use the criteria described in Subsection 11.4.

試験者は 11.4 節に記述されているクライテリアを使用しなければならない。

11.2.2.Exploitation of invalid security boundary of optical channel

Test 1: Back-flash attack

Target of test

A set of the QKD transmitter and the QKD receiver that used in TOE

TOE に使用されている QKD 送信機と受信機の 1 セット

Test equipment and configuration

- QKD transmitter (TOE)
- QKD receiver (TOE)
- Optical circulator
- Wavelength division multiplexing (WDM) filter
- Single photon detector (SPD)

－QKD 送信機

－OKD 受信機

—光サーキュレータ

—波長分割多重化フィルタ

—単一光子検出器

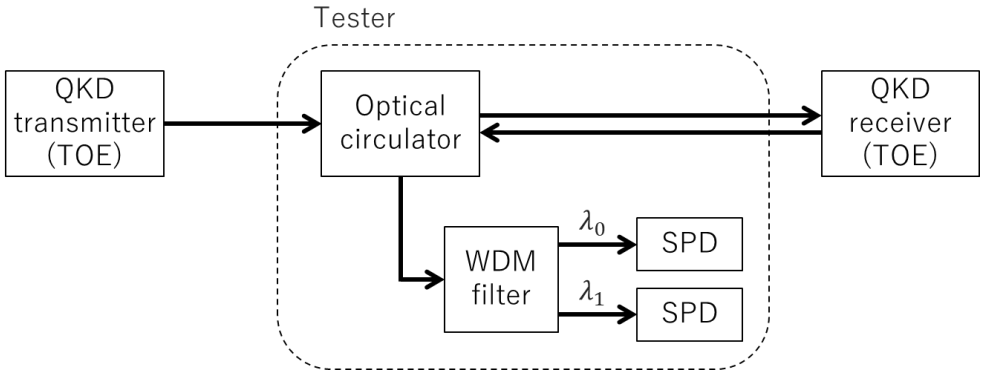

Figure 11-2 Test configuration for Back-flash Attack

Test method

The following is the procedure when the wavelength of backflash light differs for each photon detector. Let $\lambda_0(\lambda_1)$ be the wavelength of the backflash light from the photon detector corresponding to bit value 0(1) in the TOE. If degrees of freedom other than wavelength differ, conduct the test by replacing the WDM filter with an element that separates the corresponding degrees of freedom.

以下はバックフラッシュ光の波長が光子検出器ごとに異なる場合の手続きである。TOE のビット値 0 (1)に対応する光子検出器からのバックフラッシュ光の波長を$\lambda_0(\lambda_1)$とする。波長以外の自由度が異なる場合には WDM フィルタを対応する自由度を分離する素子に置き換えて試験を実施する。

Step 1. Establish a QKD link.

QKD リンクを確立する。

Step 2. During an M-round QKD session, the tester uses a circulator, WDM filter, and photon detectors to detect return light from the QKD receiver and record the bit value. The WDM filter can separate λ_0 and λ_1, and when a photon is detected by the photon detector connected to the output port corresponding to $\lambda_0(\lambda_1)$ of the WDM filter, a bit value of 0(1) is assigned.

試験者は、Mラウンドからなる QKD セッション中にサーキュレータ、WDM フィルタ、単一光子検出器を用いて QKD 受信機からの戻り光を検出し、ビット値を記録する。WDM フィルタはλ_0とλ_1を分離できるものとし、WDM フィルタの$\lambda_0(\lambda_1)$に対応する出力ポートに接続されている単一光子検出器で光子が検出された場合にはビット値 0(1)を割り当てる。

Acceptance criteria

The tester shall use the criteria described in Subsection 11.4.

試験者は 11.4 節に記載されているクライテリアを使用しなければならない。

Test 3: Trojan horse attack

The following procedure is used when the TOE decoy-state BB84 protocol generates sifted keys from the Z-basis only and the X-basis is only used to monitor eavesdropping.

TOE の decoy-state BB84 プロトコルが Z 基底のみからシフト鍵を生成し、X 基底が盗聴の監視のみに使用される場合、以下の手順が使用される。

Step 1. The tester prepares a light source (probe light source, henceforth) for probing the internal state of the QKD receiver to learn its choices of the basis.

試験者は、QKD 受信機の内部状態をプローブして、その基底の選択を把握するための光源（以下プローブ光源）を用意する。

Step 2. For each of the M rounds comprising a QKD session, the tester shall inject light from the probe light source to the QKD receiver and make a measurement on the reflected light to obtain an outcome (probe outcome, henceforth) . Then, depending on the outcome, the tester shall choose one from the following options.

QKD セッションを構成するMラウンドのそれぞれについて、試験者はプローブ光源から QKD 受信機に光を注入し、反射光を測定して結果（プローブ結果、以下）を取得しなければならない。次に、結果に応じて、試験者は以下のオプションから 1 つを選択する。

i) Measure the encoded pulse(s) the QKD transmitter sends out for the round on the Z basis. If the bit value was successfully determined, send the corresponding bright encoded pulse on the Z-basis to the QKD receiver. Otherwise, sends no light to the QKD receiver.

Note that this option is effective if, from the probe outcome, it is highly probable that the QKD receiver chose the Z-basis.
QKD 送信機がラウンドで送信する符号化パルスを Z 基底で測定する。ビット値が正常に決定された場合、対応する明るい符号化パルスを Z 基底で QKD 受信機に送信する。そうでない場合は、QKD 受信機に光を送信しない。
このオプションは、プローブの結果から、QKD 送信機が Z 基底を選択した可能性が高い場合に有効であることに注意すること
ii) Block the encoded pulse(s) the QKD transmitter sends out for the round and sends no light to the QKD receiver.
QKD 送信機がそのラウンドで送信する符号化パルスをブロックし、QKD 受信機には光を送信しない。

Step 3. After following the procedure described in one of the above options, the tester shall determine a bit value which is more likely and record it.
試験者は上記のオプションのひとつを実施した後、可能性が高いビット値を決定し記録する。

Acceptance criteria
The tester shall use the criteria described in Subsection 11.4.
試験者は 11.4 節に記載されているクライテリアを使用しなければならない。

11.2.3.Exploitation of single photon sensitivity attack

Test 1: Bright illumination attack
Target of test
A set of the QKD transmitter and the QKD receiver that used in TOE
TOE に使用されている QKD 送信機と受信機の 1 セット

Test equipment and configuration
- QKD transmitter (TOE)
- QKD receiver (TOE)
- QKD receiver (Tester)
- Laser for blind
- Laser for control
- State modulator
- Optical coupler

- QKD 送信機（TOE）
- QKD 受信機（TOE）
- QKD 受信機（試験機）
- Blind 用レーザ
- Control 用レーザ
- ステートモジュレータ
- 光カプラ

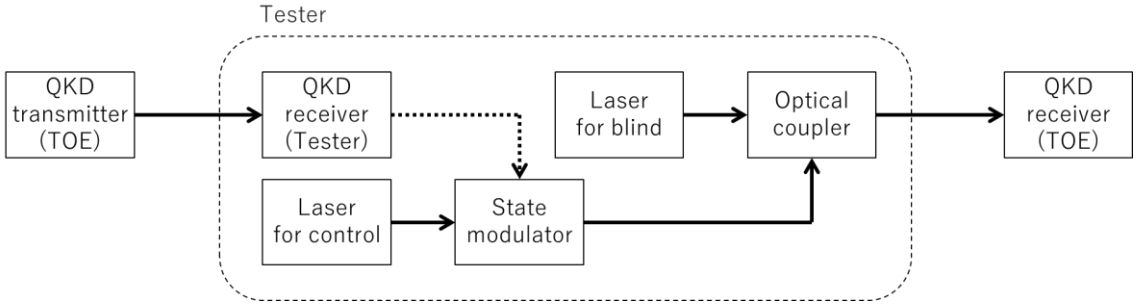

Figure 11-3 Test configuration for Bright Illumination Attack

Test method

The following procedure is used when the TOE decoy BB84decoy state BB84 protocol generates sifted keys from the Z-basis only and the X-basis is only used to monitor eavesdropping.

The tester chooses the rate t at which the bright light attack is conducted. During a QKD session consisting of M rounds, select Mt rounds and carry out the following attacks for each round

Step 1. The tester measures the optical pulses transmitted from the QKD transmitter (TOE) using the QKD receiver (Tester) in the Z-basis and records the bit values.

Step 2. The tester uses the laser for Control and the State modulator to generate optical pulse based on the bit values in Step 1.

Step 3. The tester injects a strong light into the QKD receiver (TOE) using the laser for Blind and the APD in the QKD receiver is changed to linear mode.

Step 4. The tester injects optical pulses for control generated in Step 2 into the APD, which has been changed to linear mode in Step 3.

以下は、TOE のデコイ BB84decoy state BB84 プロトコルが、Z 基底のみからシフト鍵を生成し、X 基底は盗聴の監視にのみ用いる場合の手続きである。

試験者は、明光を照射する攻撃を実施する割合tを選ぶ。Mラウンドからなる QKD セッション中、Mtラウンドを選び、各ラウンドについて以下の攻撃を行う。

Step 1. 試験者は、QKD 受信機(Tester)を用いて QKD 送信機(TOE)から送信された光パルスを Z 基底で測定し、ビット値を記録する。

Step 2. 試験者は Control 用レーザとステートモジュレータを用い、Step 1 のビット値に基づいてコントロール用の光パルスを生成する。

Step 3. 試験者は Blind 用レーザを用いて QKD 受信機(TOE)に強い光を入射し、QKD 受信機内の APD をリニアモードに移行させる。

Step 4. 試験者は Step 3 でリニアモードに移行した APD に対し、Step 2 で生成したコントロール用の光パルスを入射する。

Acceptance criteria

The tester shall use the criteria described in Subsection 11.4.

試験者は 11.4 節に記載されているクライテリアを使用しなければならない。

11.2.4.Exploitation of inaccuracy in demodulation

Test 1: Intercept-resend attack on the monitoring basis

(*Tentative*)

The following procedure is used when the TOE decoy-state BB84 protocol generates sifted keys from the Z-basis only and the X-basis is only used to monitor eavesdropping.

TOE デコイ BB84 プロトコルが Z 基底のみから選択された鍵を生成し、X 基底が傍受の監視のみに使用される場合、以下の手順が使用される。

The tester shall in advance determine the two orthogonal modes that are distinguished in the nominal X-basis measurement of the QKD receiver. The basis formed by the two modes is called X'-basis henceforth.

試験者は、QKD 受信機の名目上の X 基底において弁別される 2 つの直交モードを事前に決定する。このモードからなる基底は、以降 X'基底と呼ばれる。

The tester shall choose the rate t at which the attack is carried out. During a QKD session consisting of M rounds, the tester shall select Mt rounds and carry out the following attacks for each round.

攻撃者は、攻撃を実施する 比率 t を選択する。M ラウンドで構成される QKD セッション中、攻撃者は Mt ラウンドを選択し、各ラウンドに対して以下の攻撃を実施する。

Step 1: The tester shall measure the pulse(s) from the QKD transmitter on the X'-basis to distinguish the two orthogonal modes.

Step 2: If the measurement at Step 1 has succeeded in the distinction, the tester shall prepare a bright pulse in the corresponding mode and send it to the QKD receiver. If a sifted key bit was produced in the round, the tester shall guess the bit value from the measurement outcome and record it.

Step 3: If the measurement at Step 1 has failed, the tester sends the vacuum to the QKD receiver.

ステップ 1. 試験者は、二つの直交モードを区別するため X'基底で QKD 送信機からのパルスを測定する。

ステップ 2. ステップ 1 の測定で区別が成功した場合、試験者は対応するモードで明るいパルスを準備し、それを QKD 受信機に送信する。ラウンドでシフト鍵ビットが生成された場合、試験者は測定結果からビット値を推測し、それを記録する。

ステップ 3. ステップ 1 の測定に失敗した場合、試験者は QKD 受信機に真空状態を送信する。

Acceptance criteria

The tester shall use the criteria described in Subsection 11.4.

試験者は 11.4 節に記載されているクライテリアを使用しなければならない。

11.2.5.Exploitation of detector dead time

Target of test

A set of the QKD transmitter and the QKD receiver that are used in TOE

TOE に使用されている QKD 送信機と受信機の 1 セット

Test equipment and configuration

- QKD transmitter (TOE)
- QKD receiver (TOE)
- Laser for blind
- State modulator
-Timing controller
- Optical coupler

- QKD 送信機（TOE）
- QKD 受信機（TOE）
- Blind 用レーザ
- ステートモジュレータ
- タイミングコントローラ
- 光カプラ

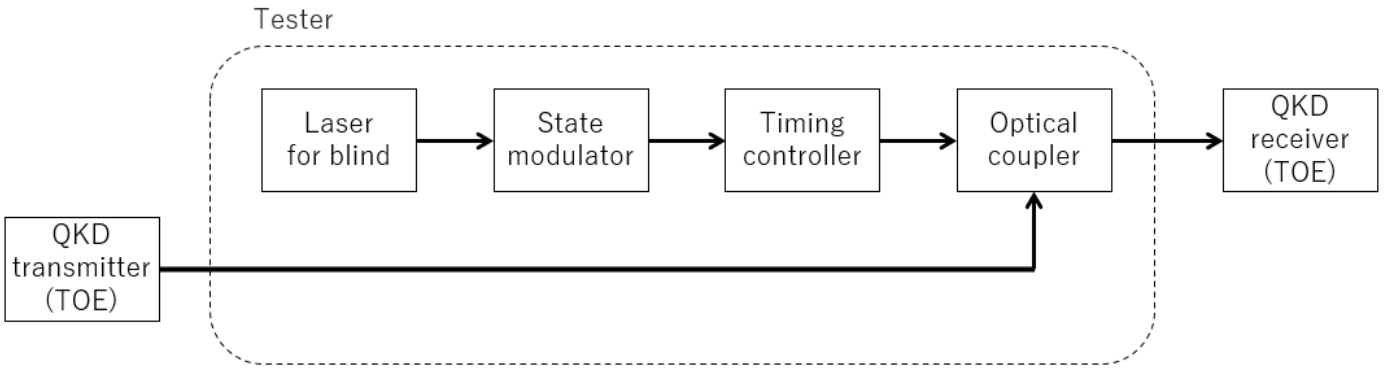

Figure 11-4 Test configuration for Detector Dead-time Attack

Test method

The following procedure is used when the TOE decoy-state BB84 protocol generates sifted keys from the Z-basis only and the X-basis is only used to monitor eavesdropping.

The tester chooses the rate t at which the bright light attack is conducted. During a QKD session consisting of M rounds, select Mt rounds and carry out the following attacks for each round

Step 1. The tester uses the laser for blind and the State modulator to generate a strong optical pulse of the state corresponding to the bit value 0 in Z-basis.

Step 2. The tester injects the optical pulse generated in Step 1 into the QKD receiver (TOE) at the time out of the detection window of the QKD receiver (TOE) to change the APD for bit value 0 in the QKD to linear mode.

Step 3. The tester records the detection events of the QKD receiver (TOE) and register the bit value of the key as 1.

Step 4. The tester uses the laser for blind and the State modulator to generate a strong optical pulse of the state corresponding to the bit value 1 in Z-basis.

Step 5. The tester injects the optical pulse generated in Step 3 into the QKD receiver (TOE) at the time out of the detection window of the QKD receiver (TOE) to change the APD for bit value 1 in the QKD to linear mode.

Step 6. The tester records the detection events of the QKD receiver (TOE) and register the bit value as 0.

以下は、TOE の decoy-state BB84 プロトコルが、Z 基底のみからシフト鍵を生成し、X 基底は盗聴の監視にのみ用いる場合の手続きである。

試験者は、明光を照射する攻撃を実施する割合tを選ぶ。Mラウンドからなる QKD セッション中、Mtラウンドを選び、各ラウンドについて以下の攻撃を行う。

Step 1. 試験者は blind 用レーザとステートモジュレータを用い、Z 基底のビット値 0 に対応する状態の強い光パルスを生成する。

Step 2. 試験者は QKD 受信機(TOE)に Step1 で生成した光パルスを入射し、QKD 受信機内のビット値 0 に対

応する APD をリニアモードに移行させる。

Step 3. 試験者は QKD 受信機(TOE)の光検出事象を記録し，鍵のビット値を 1 とする。

Step 4. 試験者は blind 用レーザとステートモジュレータを用い、Z 基底のビット値 1 に対応する状態の強い光パルスを生成する。

Step 5. 試験者は QKD 受信機(TOE)に Step1 で生成した光パルスを入射し、QKD 受信機内のビット値 1 に対応する APD をリニアモードに移行させる。

Step 6. 試験者は QKD 受信機(TOE)の光検出事象を記録し，鍵のビット値を 0 とする。

Acceptance criteria

The tester shall use the criteria described in Subsection 11.4.

試験者は 11.4 節に記載されているクライテリアを使用しなければならない。

11.3. Whole of the TOE

11.3.1.Exploitation of invalid calibration

The object to be calibrated and the method of calibration vary from device to device. The tester should obtain information on TOE calibration and structure the test accordingly. As a simple example, this SD will treat the case where the polarization is loaded with information and the detection timing is adjusted for each polarization.

キャリブレーションを行う対象と方法は装置によって異なる．試験者は TOE のキャリブレーションに関する情報を入手し，それに基づいて試験を構成すべきである．ここではわかりやすい例として偏光に情報が載せられており，それぞれの偏光に対して検出タイミングを調整する場合を扱う．

Target of test

A set of the QKD transmitter and the QKD receiver that are used in TOE

TOE に使用されている QKD 送信機と受信機の 1 セット

Test equipment and configuration

- QKD transmitter (TOE)
- QKD receiver (TOE)
- Polarization beam splitter
- Optical delay
- Polarization beam combiner
- QKD 送信機（TOE）
- QKD 受信機（TOE）
- 偏光ビームスプリッタ
- 光カプラ
- 偏光ビームコンバイナ

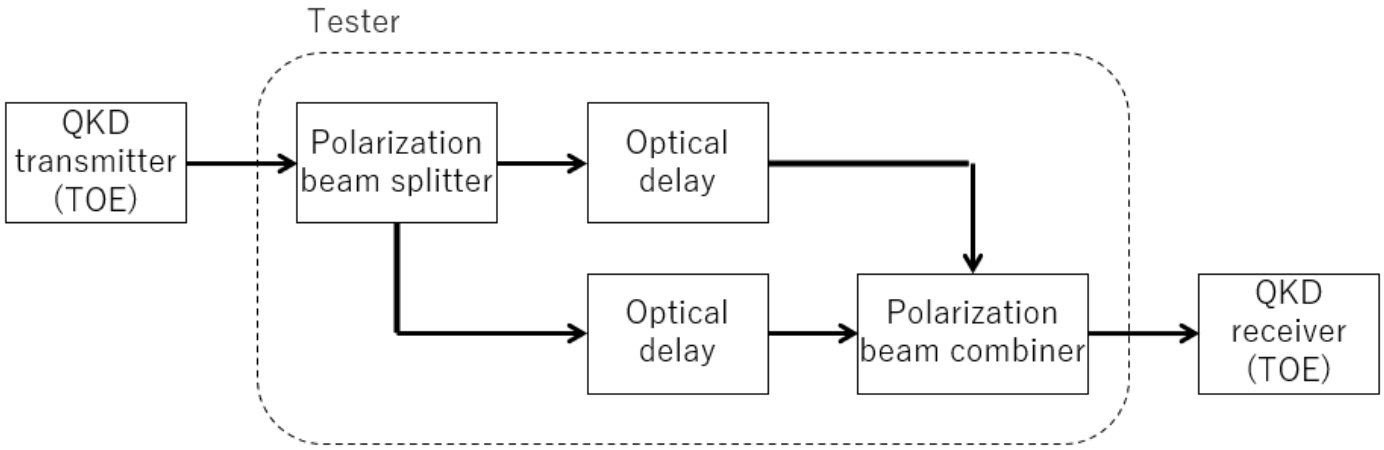

Figure 11-5 Test configuration for Invalid Calibration

Test method

The following procedure is used when the TOE decoy-state BB84 protocol generates sifted keys from the Z-basis only and the X-basis is only used to monitor eavesdropping. The bit value 0 and 1 are assigned to be horizontal and vertical polarization states, respectively. This assignment can be altered.

Step 1 In the calibration process, the tester sets a value for difference of optical delays, which should be determined to maximize the difference of the photon detectors.

Step 2 In the key generation process, the tester sets the optical delays to yield the same delay value. Then, the test proceeds Time-shift Attack which is described in Subsubsection 10.9.2.2 (see also reference below).

TOE decoy-state BB84 プロトコルが Z 基底のみからシフト鍵を生成し、X 基底は盗聴の監視にのみ使用される場合、以下の手順が使用される。ビット値 0 と 1 はそれぞれ水平偏波状態と垂直偏波状態に割り当てられる。この割り当ては変更可能である。

ステップ 1 校正プロセスでは、試験者は光遅延の差の値を設定する。この値は、光子検出器の差が最大になるように決定される。

ステップ 2 鍵生成プロセスでは、試験者は同じ遅延値になるように光遅延を設定する。その後、10.9.2.2 に記述されているタイムシフト攻撃を行う（下記も参照のこと）。

Reference

Yi Zhao, Chi-Hang Fred Fung, Bing Qi, Christine Chen, and Hoi-Kwong Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems", Phys. Rev. **A 78,** 042333 (2008)

11.4. Acceptance criteria

Parameters, variables and functions are defined as follows:

α : Pre-defined significance level per single main test

ϵ : Security parameters set in the above QKD session

$\boldsymbol{\kappa}_{\mathrm{sif}}, N$: Sifted key and its lengths generated by the TOE in the above QKD sessions.

$\boldsymbol{\kappa}_{\mathrm{QKD}}, K$: QKD key generated by the TOE in the above QKD session and its length.

f_{PA} : The hush function used by TOE for privacy amplification in the above QKD session

N_1 : Number of rounds in which a bit value is recorded in the attack and a sifted key bit is generated by the TOE.

$\boldsymbol{\kappa}_{1,\mathrm{att}}$: The N_1-bit string consisting of the bit values recorded in the above N_1 rounds.
N_{EC} : Number of bits transmitted by the TOE for error correction in the above QKD session.
$\mathrm{wt}(\boldsymbol{b})$: Number of '1's in bitstring $\boldsymbol{b}$
$H(x) \coloneqq -x\ \log_2 x - (1-x)\log_2(1-x)$: binary entropy function

The tester chooses the largest possible non-negative integer N_{err} to satisfy the following condition.

$$N_1 H(N_{\mathrm{err}}/N_1) + (N - N_1) \leq K + N_{\mathrm{EC}} + \log_2(\alpha - \epsilon)$$

However, if the information transmitted by the TOE for error correction is encrypted and the formula for determining the QKD key length after privacy amplification does not include N_{EC}, the above inequality with $N_{\mathrm{EC}} = 0$ is used instead.
Note that if there is no non-negative integer N_{err} satisfying the condition, the attack fails.

The tester determines the success or failure of the attack in one of the following ways

(1) Take the sifted key $\boldsymbol{\kappa}_{\mathrm{sif}}$ from the TOE and extract the bits corresponding to the N_1 rounds in which the above attack was conducted to form the N_1 bit sequence $\boldsymbol{\kappa}_{1,\mathrm{sif}}$. The attack is successful if $\mathrm{wt}\left(\boldsymbol{\kappa}_{1,\mathrm{att}} - \boldsymbol{\kappa}_{1,\mathrm{sif}}\right) \leq N_{\mathrm{err}}$. If not satisfied, the attack fails.

(2) Take the QKD key $\boldsymbol{\kappa}_{\mathrm{QKD}}$ from the TOE. The sifted key $\boldsymbol{\kappa}_{\mathrm{sif}}$ actually generated by the TOE is not used. For an N-bit string $\boldsymbol{\kappa}$, let $f_1(\boldsymbol{\kappa})$ be the N_1-bit string formed by concatenating the bits corresponding to the N_1 rounds. The attack is successful if there exists an N-bit string $\boldsymbol{\kappa}$ that satisfies $f_{\mathrm{PA}}(\boldsymbol{\kappa}) = \boldsymbol{\kappa}_{\mathrm{QKD}}$ and $\mathrm{wt}\left(\boldsymbol{\kappa}_{1,\mathrm{att}} - f_1(\boldsymbol{\kappa})\right) \leq N_{\mathrm{err}}$. The attack fails if there are no such strings.

Notes

If the QKD key has ϵ-security, then the probability of the successful attack is lower than α under the above decision conditions.
In choosing the rate t at which to carry out the attack, note that as t is increased, N_1 increases, but K decreases due to an increase in bit errors in the X-basis.

以下の様にパラメータ、変数、関数を定義する：
α：あらかじめ設定された本試験 1 回あたりの有意水準
ϵ：上記の QKD セッションで設定されたセキュリティパラメータ
$\boldsymbol{\kappa}_{\mathrm{sif}}, N$ ： 上記の QKD セッションで TOE が生成したシフト鍵とその長さ
$\boldsymbol{\kappa}_{\mathrm{QKD}}, K$ ： 上記の QKD セッションで TOE が生成した QKD 鍵とその長さ
f_{PA} ： 上記の QKD セッションで TOE が秘匿性増強に用いたハッシュ関数
N_1 ： 攻撃によりビット値が記録され、かつ、TOE がシフト鍵ビットを生成したラウンドの数
$\boldsymbol{\kappa}_{1,\mathrm{att}}$ ： 上記のN_1ラウンドにおいて、記録されたビット値から構成したN_1ビット列
N_{EC} ： 上記の QKD セッションでエラー訂正のために TOE が送信したビット数
$\mathrm{wt}(\boldsymbol{b})$: ビット列$\boldsymbol{b}$に含まれる‘1’の数
$H(x) \coloneqq -x\ \log_2 x - (1-x)\log_2(1-x)$ ： バイナリエントロピー関数

試験者は、次の条件を満たすように、できるだけ大きい非負の整数N_{err}を選ぶ。

$$N_1 H(N_{\mathrm{err}}/N_1) + (N - N_1) \leq K + N_{\mathrm{EC}} + \log_2(\alpha - \epsilon)$$

ただし、エラー訂正のために TOE が送信した情報が暗号化され、秘匿性増強後の QKD 鍵長を決定する公式がN_{EC}を含まない場合は、上記不等式で$N_{\mathrm{EC}}=0$としたものを替わりに用いる。
なお、条件を満たす非負の整数N_{err}が存在しなければ攻撃は失敗である。

試験者は、以下のいずれかの方法で侵入テストの攻撃の成否を判定する。
（1）TOE からシフト鍵$\boldsymbol{\kappa}_{\mathrm{sif}}$を取り出し、上記の攻撃が実施された$N_1$ラウンドに対応するビットを抜きだして$N_1$ビット列$\boldsymbol{\kappa}_{1,\mathrm{sif}}$を構成する。$\mathrm{wt}\left(\boldsymbol{\kappa}_{1,\mathrm{att}}-\boldsymbol{\kappa}_{1,\mathrm{sif}}\right)\leq N_{\mathrm{err}}$を満たしていれば攻撃は成功。満たさなければ攻撃は失敗。
（2）TOE から QKD 鍵$\boldsymbol{\kappa}_{\mathrm{QKD}}$を取り出す。TOE が実際に生成したシフト鍵$\boldsymbol{\kappa}_{\mathrm{sif}}$は用いない。$N$ビット列$\boldsymbol{\kappa}$に対し、$N_1$ラウンドに対応するビットを抜きだした$N_1$ビット列を$f_1(\boldsymbol{\kappa})$とする。$f_{\mathrm{PA}}(\boldsymbol{\kappa})=\boldsymbol{\kappa}_{\mathrm{QKD}}$かつ$\mathrm{wt}\left(\boldsymbol{\kappa}_{1,\mathrm{att}}-f_1(\boldsymbol{\kappa})\right)\leq N_{\mathrm{err}}$を満たす$N$ビット列$\boldsymbol{\kappa}$が存在すれば攻撃は成功。そのようなビット列が存在しなければ攻撃は失敗。

Notes
QKD 鍵がϵ-セキュリティを持つなら、上記の判定条件で攻撃が成功となる確率はα以下である。

攻撃を実施する割合tの選択においては、tを大きくすると、N_1は大きくなるが、X 基底におけるビットエラーが増加するためKが減少することに留意する。

12. Calculating attack potential

The evaluator shall calculate the attack potential according to [CEM] Appendix B.6. This section presents specific interpretations of attack potential calculations for the evaluation of QKD protocol implementation.
評価者は、[CEM] 附属書 B.6 に従って攻撃力を計算しなければならない)。この章では、QKD プロトコル実装評価に固有の攻撃力計算の解釈について説明する。

1. Elapsed Time

For FCS_QKD.1, the time required to overturn assumptions in security proofs. If the assumption(s) are overturned, QKD protocol cannot enforce its security proof, the security parameters in FCS_QKD.1.1 is not maintained, and FCS_QKD.1 is violated. Logically, this elapsed time is almost equal to the time it takes to fail the penetration test in Section 11. In many cases, violations of this SFR are accompanied by violations of FPT_EMS.1 and FPT_PHP.1. It is not required to consider the elapsed time until disclosure of the QKD key. The QKD key is of indefinite length, and hence if QKD protocol is run continuously, the elapsed time become infinite. Or the elapsed time for a length 2L QKD key is twice of the elapse time for a length L QKD key. That is, the elapsed time until disclosure of the QKD key only represent the QKD key length. If vulnerabilities are identified against other SFRs, the elapsed time is as defined in [CEM].
FCS_QKD.1 に関しては、セキュリティ証明の仮定を覆すのに必要な時間。仮定が覆されると、QKD プロトコルはセキュリティ証明を実施できなくなり、FCS_QKD.1.1 のセキュリティパラメータは維持されず、FCS_QKD.1 は侵害される。論理的には、この所要時間は、11 章の侵入テストに FAIL するまでの時間とほぼ等しい。多くの場合、この SFR 侵害は、FPT_EMS.1 や FPT_PHP.1 の侵害を伴う。
QKD 鍵暴露までの所要時間を考慮する必要はない。QKD 鍵の長さは不定であり、もし、QKD プロトコルを継続的に実行すると、その所要時間は無限になる。あるいは、長さ 2L の QKD 鍵の為の所要時間は、長さ L の QKD 鍵の為の所要時間の 2 倍である。つまり、QKD 鍵暴露までの所要時間は、QKD 鍵の長さを表現するだけである。脆弱性が他の SFR に対して識別された場合、所要時間は[CEM]で定義されている通りである。

2. Specialist Expertise

The specialist expertise is as defined in [CEM]. Attack methods against QKD protocol implementations require optimization of attack methods based on knowledge of the QKD protocol and the implementation structures. At last, experts-level knowledge is required for the known vulnerabilities identified in Section 9.
専門知識は、[CEM]で定義されている通りである。QKD プロトコル実装に対する攻撃手法は、QKD プロトコルと実装構造の知識に基づいて攻撃手法を最適化する必要がある。少なくとも 9 章で識別された公知の脆弱性については、エキスパートレベルの知識が必要である。

3. Knowledge of the TOE

The knowledge of the TOE is as defined in [CEM].
TOE の知識は、[CEM]で定義されている通りである。

4. Window of opportunity

The window of opportunity is as defined in [CEM]. At least for the known vulnerabilities identified in Section 4, attackers can attempt attacks by accessing the QKD link that are located in public area. Therefore, the attack opportunity is "unlimited".

機会は、[CEM]で定義されている通りである。少なくとも 4 章で識別された公知の脆弱性については、攻撃者は公共エリアにある QKD リンクにアクセスして攻撃を試みることができる。従って、攻撃機会は「無制限」である。

5. IT hardware/software or other equipment

The equipment is as defined in [CEM]. For example, equipment which may be required for attack methods identified in Section 4 are classified as follows. This guide is based on price of each equipment.
機器は、[CEM]で定義されている通りである。例えば、4 章で識別された攻撃方法に必要かも知れない機器は、次の様に分類される。このガイドは、各機器の価格に基づいている。

Table 12-1 List of equipment

Classification	Equipment
Standard	Optical amplifier 光増幅器
	Photodetector フォトディテクタ
	Optical power meter 光パワーメータ
	Polarization analyser 偏光アナライザ
	Beam splitter ビームスプリッタ
	Polarizing beam splitter 偏光ビームスプリッタ
	Circulator サーキュレータ
	Delay interferometer 遅延干渉計
	Optical delay line 光遅延器
	Polarization controller 偏光コントローラ
	Phase modulator 位相変調器
	Intensity modulator 強度変調器
	Variable Optical Attenuator 可変光減衰器
Specialised	Tuneable laser 波長可変レーザ
	Photon detector 単一光子検出器
	High-end oscilloscope ハイエンドオシロスコープ
	Optical spectrum analyser 光スペクトラムアナライザ
	Spectrum analyser スペクトラムアナライザ
	Time interval analyser タイムインターバルアナライザ

6. Example of ratings

In typical cases, expected rating for the known vulnerabilities identified in Section 4, the rating is shown below.
典型的な場合、4 章で識別された公知の脆弱性の予想されるレーティングは次の通り。

Table 12-2 Example of ratings

Elapsed Time	<= 2weeks	2	In situations where an attack is successful, the elapsed time is not so long. If we estimate longer, it is two weeks. 攻撃が成功する状況では、所要時間はそれほど長くない。長めに見積もったとし

			ても、２週間である。
Specialist Expertise	experts	6	As in 2, the typical rating is experts. 2 のように、典型的なレートはエキスパートである。
Knowledge of the TOE	public	0	As in 3, the typical rating is public. 3 のように、典型的なレートは公開である。
Window of opportunity	unlimited	0	As in 4, the typical rating is unlimited. 4 のように、典型的なレートは無制限である。
Equipment	specialised	4	As in 5, the typical rating is specialised. 5 のように、典型的なレートは特殊である。
Total		12	

13. Rationale for waiving penetration test

13.1. QKD transmitter

At the moment, no rationale for waving penetration test has been provided in the context of vulnerability analysis on the QKD transmitter.

現在、QKD 送信機における脆弱性分析の文脈において、侵入テストを免除する根拠は提示されていない。

13.2. QKD receiver

13.2.1.Detection efficiency

Rationale: Success conditions for penetration tests exploiting detector efficiency mismatch

This section deals with a penetration test with attacks exploiting difference in the detection efficiencies between the two photon detectors for bit values 0 and 1 used for generation of sifted key bits on the Z basis. Although this section assesses the threat caused by innate efficiency mismatch, this rationale is written such to also address cases where the mismatch arises from adversary intervention affecting the degrees of freedom of the optical pulses in the quantum channel, as detailed in Subsection 9.2.1.

このセクションでは、Z 基盤のシフト鍵ビット生成に使用されるビット値 0 と 1 に対する 2 つの光子検出器の検出効率の差を利用した攻撃による侵入テストについて取り扱う。このセクションでは、生来の効率の不整合による脅威を評価するが、詳細は第 9.2.1 節で説明されているように、この根拠は量子チャネルにおける光パルスの自由度に影響を与える敵対的な介入により不一致が生じる場合にも対応するように記述されている。

In the following, the probability for the TOE to fail the penetration test is estimated using conditions obtained from functional tests and using a set of plausible assumptions. A concise sufficient condition for the failing probability to be negligibly small is given. Here we consider a decoy-state BB84 protocol in which the sifted key is generated from the Z basis only and the X basis is only used to monitor eavesdropping. The basis selection used in the QKD receiver may be an active or a passive one.

以下では、機能テストから得られた条件と、妥当な仮定のセットを使用して、TOE が侵入テストに不合格となる確率を推定する。不合格確率が十分に小さいという簡潔な十分条件が与えられる。ここでは、シフト鍵が Z 基底のみから生成され、X 基底は盗聴の監視にのみ使用される、decoy-state BB84 プロトコルを考える。QKD 受信機で使用される基底選択は能動的なものでも受動的なものでもよい。

Suppose that a penetration test is conducted on a QKD session. Define parameters, variables, and functions as follows:

QKD セッションで侵入テストが実施されたと仮定する。パラメータ、変数、関数を以下のように定義する。

M : Number of communication rounds in the QKD session

QKD セッションにおける通信ラウンド数

$\bar{\mu}$: The mean photon number in a pulse (or a pair of pulses), averaged over the Z-basis signals.

Z 基底の信号について平均した、1 パルス(あるいはパルス対)に含まれる平均光子数

$Q_{Z0(1)}$: Probability for a round to produce a sifted key bit with a bit value 0(1)

ビット値 0(1)のシフト鍵ビットが 1 ラウンドで生成される確率

N : Length of the sifted key produced in the QKD session

QKD セッションで生成されたシフト鍵の長さ

$\boldsymbol{b}$: N-bit sifted key produced in the QKD session

QKD セッションで生成された N ビットのシフト鍵

K : Length of the QKD key produced in the QKD session
QKD セッションで生成された QKD 鍵の長さ
N_{EC} : Length of the bit strings communicated for the error reconciliation that is accounted for in the privacy amplification. If the string is encrypted and is not accounted for in the privacy amplification, assume $N_{\mathrm{EC}} = 0$.
秘匿増強で考慮されるエラー調整のために通信されるビット列の長さ。ビット列が暗号化され、秘匿増強で考慮されない場合は、$N_{\mathrm{EC}} = 0$とみなす。
$H(x) \coloneqq -x\ \log_2 x - (1-x)\log_2(1-x)$: Binary entropy function　二値エントロピー関数
$D(x||y) \coloneqq x\ \log_2 \frac{x}{y} + (1-x)\log_2 \frac{1-x}{1-y}$: Kullback–Leibler divergence　カルバック・ライブラー情報量
$\mathrm{wt}(\boldsymbol{a})$: Number of '1's in bit string $\boldsymbol{a}$.
ビット列$\boldsymbol{a}$中の'1'の数
This rationale takes the following assumptions. These assumptions are expected to be true for penetration tests in Subsubsection. 11.2.1, but the evaluator should confirm the validity of them before applying this Rationale.
この理論的根拠は、以下を仮定としている。これらの前提は、11.2.1 項の侵入テストでは正しいと予想されるが、評価者はこの根拠を適用する前に、それらの妥当性を確認すべきである。

(A1) The criteria for the TOE to fail the penetration test is given as direct or indirect confirmation of the N-bit sifted key $\boldsymbol{b}$ belonging to a predicted set $\Omega \subset \{0,1\}^N$ satisfying $|\Omega| \leq 2^{K+N_{\mathrm{EC}}}$.
TOE が侵入テストに不合格となる基準は、$|\Omega| \leq 2^{K+H_{\mathrm{EC}}}$満たす予測された集合$\Omega \subset \{0,1\}^N$に$N$ビットのシフト鍵$\boldsymbol{b}$が属するかどうかの直接または間接的に確認である。
(A2) The privacy amplification ratio determined by the TOE correctly accounts for the fact that a sifted key bit may have leaked completely if the signal emitted from the transmitter included multiple photons.
TOE によって決定される秘匿増強率は、送信機から放出された信号に複数の光子が含まれていた場合、シフト鍵ビットが完全に漏洩していた可能性があるという事実を正確に考慮している。
(A3) The probability for the TOE to produce a sifted key bit when the transmitter emits two or more photons in an optical mode is no lower than that when it emits one or no photon in the same mode.
送信機が 2 つ以上の光子をある光モードで放出する場合、TOE がシフト鍵ビットを生成する確率は、同じモードで 1 つまたは 0 個の光子を放出する場合の確率よりも低くはない。
(A4) The photon number distribution in a signal emitted from the transmitter is well approximated by a Poisson distribution.
送信機から放出される信号の光子数分布は、ポアソン分布でよく近似される。
(A5) The mean photon number in every signal emitted from the transmitter does not exceeds unity.
送信機から放出される信号の平均光子数は、1 を超えない。
In each round of a QKD session, the attacker may attack on the optical pulse(s) to modify the probabilities Q_{Z0} and Q_{Z1}. Suppose that a functional test assures that

$$\frac{\gamma}{1-\gamma} \leq \frac{Q_{Z1}}{Q_{Z0}} \leq \frac{1-\gamma}{\gamma}$$

holds for a positive constant $\gamma \leq 1/2$. Note that Q_{Z0} and Q_{Z1} may be different for different rounds.
QKD セッションの各ラウンドにおいて、攻撃者は光パルスを攻撃して確率Q_{Z0}およびQ_{Z1}を変更することがある。機能テストにより、

$$\frac{\gamma}{1-\gamma} \leq \frac{Q_{Z1}}{Q_{Z0}} \leq \frac{1-\gamma}{\gamma}$$

が正の定数$\gamma \leq 1/2$に対して成り立つことが保証されていると仮定する。Q_{Z0}とQ_{Z1}はラウンドごとに異なる可能性があることに注意すること。

Suppose that after the QKD session, the QKD receiver has produced a sifted key $\boldsymbol{b}$ of length N from a specific set of N rounds. On condition of those locations of the N rounds, we consider the conditional probability of the N-bit string $\boldsymbol{b} = b^{[1]} \cdots b^{[N]}$ over the 2^N values. Each bit is independent of the others, and $\mathrm{Prob}\{b^{[j]} = c\} = Q_{Zc}/(Q_{Z0} + Q_{Z1})$ where the values of Q_{Z0} and Q_{Z1} are for the round at which the jth sifted key bit $b^{[j]}$ was produced. Define a constant bit $c^{[j]}$ by $c^{[j]} = 0$ for $Q_{Z0} \geq Q_{Z1}$ and $c^{[j]} = 1$ for $Q_{Z0} < Q_{Z1}$. Then we have

$$p^{[j]} \coloneqq \mathrm{Prob}\{b^{[j]} \neq c^{[j]}\} = 1 - \frac{Q_{Zc^{[j]}}}{(Q_{Z0} + Q_{Z1})} \geq \gamma,$$

and hence the expectation value of $\mathrm{wt}(\boldsymbol{b} - \boldsymbol{c})$ is no smaller than γN. From Hoeffding's inequality, we have, for all $\delta > 0$,

$$\mathrm{Prob}\{\mathrm{wt}(\boldsymbol{b} - \boldsymbol{c}) \leq (\gamma - \delta)N\} \leq \exp(-2\delta^2 N).$$

On the other hand, for any N-bit string $\boldsymbol{\Delta}$ with $\mathrm{wt}(\boldsymbol{\Delta}) \geq (\gamma - \delta)N$,

$$\mathrm{Prob}\{\boldsymbol{b} - \boldsymbol{c} = \boldsymbol{\Delta}\} \leq \gamma^{(\gamma-\delta)N}(1-\gamma)^{(1-\gamma+\delta)N} = 2^{-N(D(\gamma||\gamma-\delta)+H(\gamma-\delta))},$$

where $D(\gamma||\gamma - \delta) > 0$. Hence, according to (A1), the probability P_{fail} for the TOE to fail the penetration test satisfies

$$\begin{aligned} P_{\mathrm{fail}} = \ & \mathrm{Prob}\{\boldsymbol{b} \in \Omega\} \\ \leq \ & \mathrm{Prob}\{\boldsymbol{b} \in \Omega, \mathrm{wt}(\boldsymbol{b} - \boldsymbol{c}) \leq (\gamma - \delta)N\} + \mathrm{Prob}\{\boldsymbol{b} \in \Omega, \mathrm{wt}(\boldsymbol{b} - \boldsymbol{c}) \geq (\gamma - \delta)N\} \\ \leq \ & e^{-2\delta^2 N} + |\Omega| 2^{-N(D(\gamma||\gamma-\delta)+H(\gamma-\delta))} \leq e^{-2\delta^2 N} + 2^{-N(D(\gamma||\gamma-\delta)+H(\gamma-\delta))+K+H_{\mathrm{EC}}}. \end{aligned}$$

Hence, if

$$H(\gamma) > \frac{K + H_{\mathrm{EC}}}{N}$$

holds, we may choose $\delta > 0$ such that $NH(\gamma - \delta) = K + H_{\mathrm{EC}}$ holds, which shows that the probability P_{fail} is negligibly small.

QKD セッションの後、QKD 受信機が特定の N ラウンドから長さ N のシフト鍵$\boldsymbol{b}$を生成したと仮定する。Nラウンドの位置を条件として、2^Nの値に対するNビット列$\boldsymbol{b} = b^{[1]} \cdots b^{[N]}$の条件付き確率を考える。各ビットは互いに独立であり、$\mathrm{Prob}\{b^{[j]} = c\} = Q_{Zc}/(Q_{Z0} + Q_{Z1})$ここで、$Q_{Z0}$と$Q_{Z1}$の値は、$j$番目のシフト鍵ビット$b^{[j]}$ が生成されたラウンドのものである。定数ビット $c^{[j]}$ を、$Q_{Z0} \geq Q_{Z1}$の場合は$c^{[j]} = 0$、$Q_{Z0} < Q_{Z1}$の場合は$c^{[j]} = 1$として定義する。次に

$$p^{[j]} \coloneqq \mathrm{Prob}\{b^{[j]} \neq c^{[j]}\} = 1 - \frac{Q_{Zc^{[j]}}}{(Q_{Z0} + Q_{Z1})} \geq \gamma,$$

したがって、$\mathrm{wt}(\boldsymbol{b} - \boldsymbol{c})$の期待値は$\gamma N$より小さくならない。Hoeffding の不等式より、$\delta > 0$の場合、

$$\mathrm{Prob}\{\mathrm{wt}(\boldsymbol{b} - \boldsymbol{c}) \leq (\gamma - \delta)N\} \leq \exp(-2\delta^2 N).$$

一方、$\mathrm{wt}(\boldsymbol{\Delta}) \geq (\gamma - \delta)N$を満たす任意の$N$ビット文字列$\boldsymbol{\Delta}$に対して、

$$\mathrm{Prob}\{\boldsymbol{b} - \boldsymbol{c} = \boldsymbol{\Delta}\} \leq \gamma^{(\gamma-\delta)N}(1-\gamma)^{(1-\gamma+\delta)N} = 2^{-N(D(\gamma||\gamma-\delta)+H(\gamma-\delta))},$$

ここで$D(\gamma||\gamma - \delta) > 0$.　したがって、(A1)によれば、TOE が侵入テストに不合格となる確率P_{fail}は、

$$\begin{aligned} P_{\mathrm{fail}} = \ & \mathrm{Prob}\{\boldsymbol{b} \in \Omega\} \\ \leq \ & \mathrm{Prob}\{\boldsymbol{b} \in \Omega, \mathrm{wt}(\boldsymbol{b} - \boldsymbol{c}) \leq (\gamma - \delta)N\} + \mathrm{Prob}\{\boldsymbol{b} \in \Omega, \mathrm{wt}(\boldsymbol{b} - \boldsymbol{c}) \geq (\gamma - \delta)N\} \\ \leq \ & e^{-2\delta^2 N} + |\Omega| 2^{-N(D(\gamma||\gamma-\delta)+H(\gamma-\delta))} \leq e^{-2\delta^2 N} + 2^{-N(D(\gamma||\gamma-\delta)+H(\gamma-\delta))+K+H_{\mathrm{EC}}}. \end{aligned}$$

したがって、

$$H(\gamma) > \frac{K + H_{\mathrm{EC}}}{N}$$

が成り立つ場合、$NH(\gamma - \delta) = K + H_{\mathrm{EC}}$が成り立つような$\delta > 0$を選択することができ、これにより、$P_{\mathrm{fail}}$の確率は無視できるほど小さいことが示される。

We may further rewrite the condition by using assumptions (A2)-(A5). Let be the number of photons in the pulse(s) sent out by the transmitter in a round. Let "*tran_Z*" denote the event where the transmitter chooses the Z basis, and "*sif_suc*" denote the event where the TOE produces a sifted key bit. Then (A2) implies that

$$N - (K + H_{\mathrm{EC}}) > N\,\mathrm{Prob}\{n \geq 2 | sif\_suc\}$$

holds except a negligibly small probability. Since (A3) implies $\mathrm{Prob}\{sif\_suc | tran\_Z,\ n \geq 2\} \geq$

$\mathrm{Prob}\{sif\_suc|tran\_Z,\ n \le 1\}$, we have $\mathrm{Prob}\{sif\_suc|tran\_Z,\ n \ge 2\} \ge \mathrm{Prob}\{sif\_suc|tran\_Z\}$ and hence

$$\mathrm{Prob}\{n \ge 2|sif\_suc\} = \mathrm{Prob}\{n \ge 2|sif\_suc, tran\_Z\} \ge \mathrm{Prob}\{n \ge 2|\ tran\_Z\}.$$

From (A4), we may write $\mathrm{Prob}\{n \ge 2|\ tran\_Z\} = \sum_i p_i f(\mu_i)$ with $f(\mu) \coloneqq 1 - e^{-\mu}(1+\mu)$. Since $f''(\mu) \ge 0$ for $0 \le \mu \le 1$, (A5) implies that, for $\bar{\mu} \coloneqq \sum_i p_i \mu_i$,

$$\mathrm{Prob}\{n \ge 2|\ tran\_Z\} \ge f(\bar{\mu}).$$

Combining all the inequalities, we conclude that the probability P_{fail} is negligibly small if

$$H(\gamma) > e^{-\bar{\mu}}(1+\bar{\mu}).$$

さらに、仮定（A2）～（A5）を用いて条件を書き換えることができる。送信機が 1 ラウンドで送信するパルス（複数可）内の光子の数をnとする。送信機が Z 基底を選択する事象を「tran_Z」とし、TOE が選別された鍵ビットを生成する事象を「sif_suc」とする。すると、(A2)は、

$$N - (K + H_{\text{EC}}) > N\ \mathrm{Prob}\{nn \ge 2|sif\_suc\}$$

が、無視できるほど小さな確率を除いて成り立つことを意味する。(A3)より、$\mathrm{Prob}\{sif\_suc|tran\_Z,\ n \ge 2\} \ge \mathrm{Prob}\{sif\_suc|tran\_Z,\ n \le 1\}$、$\mathrm{Prob}\{sif_suc|tran_Z,\ n \ge 2\} \ge \mathrm{Prob}\{sif_suc|tran_Z\}$が成り立ち、したがって

$$\mathrm{Prob}\{n \ge 2|sif\_suc\} = \mathrm{Prob}\{n \ge 2|sif\_suc, tran\_Z\} \ge \mathrm{Prob}\{n \ge 2|\ tran\_Z\}.$$

(A4)より、$\mathrm{Prob}\{n \ge 2|\ tran\_Z\} = \sum_i p_i f(\mu_i)$ with $f(\mu) \coloneqq 1 - e^{-\mu}(1+\mu)$と書くことができる。$0 \le \mu \le 1$に対して$f''(\mu) \ge 0$であるため、（A5）は、$\bar{\mu} \coloneqq \sum_i p_i \mu_i$に対して、

$$\mathrm{Prob}\{n \ge 2|\ tran\_Z\} \ge f(\bar{\mu}).$$

すべての不等式を組み合わせると、

$$H(\gamma) > e^{-\bar{\mu}}(1+\bar{\mu}).$$

のときP_{fail}の確率は無視できるほど小さいと結論づけられる。

13.2.2.Single-photon sensitivity

Rationale: Success conditions for penetration test of bright illumination attacks.

根拠：明光攻撃の侵入テストの成功条件について

This section deals with the bright illumination attack of the type 2).

このセクションでは、タイプ 2）の明光攻撃を扱う。

In the following, the probability for the TOE to fail the penetration test is estimated using conditions obtained from functional tests and using a set of plausible assumptions. A concise sufficient condition for the failing probability to be negligibly small is given. Here we consider a decoy-state BB84 protocol in which the sifted key is generated from the Z basis only and the X basis is only used to monitor eavesdropping. The basis selection used in the QKD receiver may be an active or a passive one. In the case of passive basis selection, the beam splitter for selecting the Z- and X-basis is assumed to have a splitting ratio favourable for the Z-basis.

以下では、TOE が侵入テストに不合格する確率を、機能テストから得られた条件と、もっともらしい仮定のセットを用いて推定する。不合格確率が無視できるほど小さくなるための簡潔な十分条件を示す。decoy-state BB84 プロトコルは、Z 基底のみからシフト鍵を生成し、X 基底は盗聴の監視にのみ用いるとする。受信装置は、能動基底選択と受動基底選択を扱う。受動選択の場合、Z 基底と X 基底を分岐するビームスプリッタの分岐比は、Z 基底側が大きいとする。

Suppose that a penetration test is conducted on a QKD session. Define parameters, variables, and functions as follows:

QKD セッションに対して侵入テストが実施されたとする。 パラメータ、変数、関数を以下のように定義する：

p_Z, p_X : Selection probabilities of the basis for the QKD transmitter

送信機の基底選択確率

r_Z, r_X : Coupling efficiency of the beam splitter for the passive basis selection of the QKD receiver

受信機の受動基底選択のビームスプリッタの結合効率

η_Z, η_X : Quantum efficiency of the two photon detectors in each base of the QKD receiver（Assume that the two have the same quantum efficiency.）
受信機の各基底の 2 個の光子検出器の量子効率（同じ量子効率を持つとする）
M : Number of communication rounds in the QKD session
QKD のセッションの通信ラウンド数。
t : Parameter indicating the frequency of Intercept-resend attacks $(0 \leq t \leq 1)$
Intercept-resend 攻撃を行う頻度を表すパラメータ$(0 \leq t \leq 1)$。
$Q_{Z(X)}$: Probability of a successful Z(X)-basis detection for a round with no intercept-resend attacks.
Intercept-resend 攻撃がないラウンドでの Z(X)基底の検出成功確率。
$\tilde{Q}_{Z(X)}$: Probability of a successful Z(X)-basis detection for a round with intercept-resend attacks.
Intercept-resend 攻撃が行われたラウンドでの Z(X)基底の検出成功確率。
N : Length of the sifted key produced in the QKD session
QKD セッション中に生成されたシフト鍵長。
$\boldsymbol{b}$: N-bit sifted key produced in the QKD session
QKD セッション中に生成された N ビットシフト鍵
K : Length of the QKD key produced in the QKD session
QKD セッション中に生成された QKD 鍵長
H_{EC} : Length of the bit strings communicated for the error reconciliation that is accounted for in the privacy amplification. If the string is encrypted and is not accounted for in the privacy amplification, assume $H_{\mathrm{EC}} = 0$.
秘匿増強で考慮されるエラー調整のために通信されるビット列の長さ。ビット列が暗号化され、秘匿増強で考慮されない場合は、$H_{\mathrm{EC}} = 0$とみなす。
$H(x) \coloneqq -x \log_2 x - (1-x)\log_2(1-x)$: Binary entropy function
二値エントロピー関数
$v(t)$: Fraction of the bits in the sifted key that could be compromised by an attacker.
シフト鍵のうち、攻撃者への漏洩があり得るビットの割合
$e(t)$: Bit error rate in the X basis.
X 基底のビットエラー率

This rationale takes the following assumptions. These assumptions are expected to be true for penetration tests in Subsection 11.2.3, but the evaluator should confirm the validity of them before applying this Rationale.
この理論的根拠は、以下を仮定としている。これらの前提は 11.2.3 項の侵入テストでは正しいと予想されるが、評価者はこの根拠を適用する前に、それらの妥当性を確認すべきである。
(A1) The criteria for the TOE to fail the penetration test is given as direct or indirect confirmation of the N-bit sifted key $\boldsymbol{b}$ belonging to a predicted set $\Omega \subset \{0,1\}^N$ satisfying $|\Omega| \leq 2^{K+H_{\mathrm{EC}}}$.
TOE が侵入テストに不合格となる基準は、Nビットのシフト鍵$\boldsymbol{b}$が予測された集合$\Omega \subset \{0,1\}^N$に属することの直接または間接的な確認であり、Ω の大きさは$|\Omega| \leq 2^{K+H_{\mathrm{EC}}}$満たす。
(A2) When the observed bit error rate in the X basis is e, the privacy amplification ratio determined by the TOE satisfies $K + H_{\mathrm{EC}} \leq N\big(1 - H(e)\big)$.
X 基底で観測されたビット誤り率をeとすると、TOE によって決定される秘匿性増強率$K + H_{\mathrm{EC}} \leq N\big(1 - H(e)\big)$が成立する。
(A3) The photon detectors may have their quantum efficiencies modified due to the bright illumination attack, they do not switch to linear mode and their response is well approximated by the standard model of an on-off detector: the detection probability when a laser pulse with average photon number μ is incident on an on-off detector with

quantum efficiency η is given by $\eta\mu\xi(\eta\mu)$, where

$$\xi(x) \coloneqq \frac{1-e^{-x}}{x}.$$

Here, $\xi(x)$ is a decreasing function and $x\xi(x)$ is an increasing function of x.

光子検出器は、明光攻撃によって量子効率が修正される可能性があるが、リニアモードに切り替わることはなく、その応答はオン・オフ検出器の標準モデルでよく近似される：量子効率ηを持つオン・オフ検出器に平均光子数μのレーザーパルスが入射したときの検出確率は以下のとき、$\eta\mu\xi(\eta\mu)$で与えられる。

$$\xi(x) \coloneqq \frac{1-e^{-x}}{x}$$

ここで、$\xi(x)$は減少関数、$x\xi(x)$はxの増加関数である。

Suppose that among the M rounds in the QKD session, an attacker performs an intercept-resend attack for Mt rounds.

QKD のセッションのMラウンド中に、攻撃者はMtラウンドについて Intercept-resend 攻撃を行うとする。

Round with no intercept-resend attack:

With probability $p_Z Q_Z$, the Z-basis communication succeeds and a sifted key bit is generated. The attacker has no knowledge of this bit value.

With probability $p_X Q_X$ the communication in the X-basis succeeds and the occurrence of a bit errors is recorded.

Intercept-resend 攻撃がないラウンド：

確率$p_Z Q_Z$で Z 基底の通信が成功し、シフト鍵が 1 ビット生成される。攻撃者はこのビット値は全く知らない。

確率$p_X Q_X$で X 基底の通信が成功し、ビットエラーの有無が記録される。

Round in which the intercept-resend attack took place:

With probability $p_Z \tilde{Q}_Z$ the communication in the Z-basis succeeds and a sifted key is generated.

With probability $p_X \tilde{Q}_X$ the communication in the X-basis succeeds and the occurrence of a bit errors is recorded. Due to the intercept-resend attack, a bit error occurs here with probability 1/2.

Intercept-resend 攻撃が行われたラウンド：

確率$p_Z \tilde{Q}_Z$で Z 基底の通信が成功し、シフト鍵が 1 ビット生成される。

確率$p_X \tilde{Q}_X$で X 基底の通信が成功し、ビットエラーの有無が記録される。Intercept-resend 攻撃のため、確率 1/2 でビットエラーが発生する。

In this QKD session,

$N = Mtp_Z \tilde{Q}_Z + M(1-t)p_Z Q_Z$ bits of sifted keys are generated, of which at least $M(1-t)p_Z Q_Z$ bits are not compromised by the attacker at all. That is, the fraction of bits in the sifted key that may be compromised is at most $v(t) \coloneqq \frac{t\tilde{Q}_Z}{t\tilde{Q}_Z + (1-t)Q_Z}$. The probability of the sifted key $\boldsymbol{b}$ to take any specific N-bit string is no greater than $2^{-N(1-v(t))}$ and hence

$$\mathrm{Prob}\{\boldsymbol{b} \in \Omega\} \leq |\Omega| 2^{-N(1-v(t))}.$$

The bit error rate observed in the X basis is at least $e(t) \coloneqq \frac{1}{2}\frac{t\tilde{Q}_X}{t\tilde{Q}_X + (1-t)Q_X}$. Hence, according to (A1) and (A2), the probability P_{fail} for the TOE to fail the penetration test satisfies

$$P_{\mathrm{fail}} = \mathrm{Prob}\{\boldsymbol{b} \in \Omega\} \leq 2^{K + H_{\mathrm{EC}} - N(1-v(t))} \leq 2^{-N(H(e(t)) - v(t))}$$

この QKD のセッションで、

$N = Mtp_Z \tilde{Q}_Z + M(1-t)p_Z Q_Z$ビットのシフト鍵が生成され、うち少なくとも$M(1-t)p_Z Q_Z$ビットは攻撃者に全く

漏洩していない。すなわち、シフト鍵中で漏洩の可能性があるビットの割合はたかだか$v(t) \coloneqq \frac{t\tilde{Q}_{\mathrm{Z}}}{t\tilde{Q}_{\mathrm{Z}}+(1-t)Q_{\mathrm{Z}}}$である。シフト鍵$\boldsymbol{b}$が特定の$N$ビット列をとる確率は$2^{-N(1-v(t))}$以下であり、したがって
$\mathrm{Prob}\{\boldsymbol{b} \in \Omega\} \leq |\Omega| 2^{-N(1-v(t))}$.が成り立つ。

X 基底で観測されるビットエラー率は、少なくとも$e(t) \coloneqq \frac{1}{2}\frac{t\tilde{Q}_{\mathrm{X}}}{t\tilde{Q}_{\mathrm{X}}+(1-t)Q_{\mathrm{X}}}$以上である。従って、(A1)と(A2)により、TOE が侵入テストに失敗する確率P_{fail}は

$$P_{\mathrm{fail}} = \mathrm{Prob}\{\boldsymbol{b} \in \Omega\} \leq 2^{K+H_{\mathrm{EC}}-N\left(1-v(t)\right)} \leq 2^{-N\left(H(e(t))-v(t)\right)}$$

Hence, if

$$H\left(e(t)\right) > v(t)$$

holds, the probability P_{fail} is negligibly small. With $t' \coloneqq 2e(t)$ and $\gamma = \frac{Q_{\mathrm{Z}}\tilde{Q}_{\mathrm{X}}}{Q_{\mathrm{X}}\tilde{Q}_{\mathrm{Z}}}$, it holds that $v(t) = \frac{t'}{t'+(1-t')\gamma}$, which leads to a necessary condition for a successful attack,

$$H\left(\frac{t'}{2}\right) < \frac{t'}{t'+(1-t')\gamma}.$$

If $\gamma > 0.285$, there is no t' in $[0,1]$ that satisfies this inequality, so the attack will fail no matter how the attack frequency t is chosen. This means that the attack in a penetration test succeeds only if it holds that

$$\gamma = \frac{Q_{\mathrm{Z}}\tilde{Q}_{\mathrm{X}}}{Q_{\mathrm{X}}\tilde{Q}_{\mathrm{Z}}} \leq 0.285.$$

従って、もし

$$H\left(e(t)\right) < v(t)$$

が成り立つとき確率P_{fail}は無視できるほど小さい。
ここで、$t' \coloneqq 2e(t)$、$\gamma = \frac{Q_{\mathrm{Z}}\tilde{Q}_{\mathrm{X}}}{Q_{\mathrm{X}}\tilde{Q}_{\mathrm{Z}}}$とおくと、$v(t) = \frac{t'}{t'+(1-t')\gamma}$が成り立つので、攻撃成功の必要条件は

$$H\left(\frac{t'}{2}\right) < \frac{t'}{t'+(1-t')\gamma}$$

となる。$\gamma > 0.285$であればこの不等式を充足するt'は$[0,1]$に存在しないので、攻撃頻度tをどのように選んでも攻撃は失敗する。つまり、侵入テストで攻撃が成功するには、少なくとも

$$\gamma = \frac{Q_{\mathrm{Z}}\tilde{Q}_{\mathrm{X}}}{Q_{\mathrm{X}}\tilde{Q}_{\mathrm{Z}}} \leq 0.285$$

が成立する必要がある。

Relation to the functional test:
From the quantum efficiencies of the detectors without bright illumination attack,

$$\frac{Q_{\mathrm{Z}}}{Q_{\mathrm{X}}} = \frac{r_Z\eta_Z}{r_X\eta_X}$$

holds. At the resending step, light with an average photon number greater than unity can also be used. When the pulse intensity incident on the QKD receiver is μ, it holds that

$$\tilde{Q}_{\mathrm{Z}} = r_Z\eta_Z\mu\xi(r_Z\eta_Z\mu)$$

according to (A3). The two photon detectors in the X-basis may have their quantum efficiencies modified due to the bright illumination attack. Denoting the modified quantum efficiencies by $\tilde{\eta}_{X0}$and $\tilde{\eta}_{X1}$, the probability of successful detection in the X basis is given by

$$\tilde{Q}_{\mathrm{X}} = \frac{r_X\tilde{\eta}_{X0}\mu}{2}\xi\left(\frac{r_X\tilde{\eta}_{X0}\mu}{2}\right) + \frac{r_X\tilde{\eta}_{X1}\mu}{2}\xi\left(\frac{r_X\tilde{\eta}_{X1}\mu}{2}\right).$$

The functional test of Sec. 10.9.2.1 guarantees that $\tilde{\eta}_{X0} \geq \kappa\,\eta_X$ and $\tilde{\eta}_{X1} \geq \kappa\,\eta_X$ using a parameter $\kappa(\leq 1)$, which takes a value close to unity. It follows that

$$\tilde{Q}_{\mathrm{X}} \geq r_X \kappa\, \eta_X \mu \xi\left(\frac{r_X \kappa\, \eta_X \mu}{2}\right),$$

which leads to

$$\gamma = \frac{Q_{\mathrm{Z}} \tilde{Q}_{\mathrm{X}}}{Q_{\mathrm{X}} \tilde{Q}_{\mathrm{Z}}} \geq\ \kappa \frac{\xi\left(\frac{r_X \kappa\, \eta_X \mu}{2}\right)}{\xi(r_Z \eta_Z \mu)}.$$

Since $\xi(x)$ is a decreasing function, $\gamma \geq \kappa$ is assured if the ratio of passive basis selection probabilities in normal operation satisfies

$$\frac{Q_{\mathrm{Z}}}{Q_{\mathrm{X}}} = \frac{r_Z \eta_Z}{r_X \eta_X} \geq \frac{1}{2}.$$

Therefore, it can be concluded that if the TOE has passed the functional test with $\kappa > 0.285$, the probability P_{fail} for the TOE to fail the penetration test is negligibly small.

機能テストとの関連付け：

明光攻撃がない場合の検出器の量子効率から、

$$\frac{Q_{\mathrm{Z}}}{Q_{\mathrm{X}}} = \frac{r_Z \eta_Z}{r_X \eta_X}$$

が成り立つ。再送信ステップでは、平均光子数が 1 より大きい光も使用できる。 QKD 受信機に入射するパルス強度を μ とすると（A3）から、

$$\tilde{Q}_{\mathrm{Z}} = r_Z \eta_Z \mu \xi(r_Z \eta_Z \mu)$$

が成り立つ。X-basis の 2 つの光子検出器は、明るい照明攻撃によって量子効率が変更される可能性がある。修正量子効率を$\tilde{\eta}_{X0}$と$\tilde{\eta}_{X1}$とすると、X 基底における検出成功確率は次式で与えられる。

$$\tilde{Q}_{\mathrm{X}} = \frac{r_X \tilde{\eta}_{X0} \mu}{2} \xi\left(\frac{r_X \tilde{\eta}_{X0} \mu}{2}\right) + \frac{r_X \tilde{\eta}_{X1} \mu}{2} \xi\left(\frac{r_X \tilde{\eta}_{X1} \mu}{2}\right)$$

第 10.7.1.1 節の機能テストは、$\tilde{\eta}_{X0} \geq \kappa\, \eta_X$ と $\tilde{\eta}_{X1} \geq \kappa\, \eta_X$ を、1 に近い値をとるパラメータ $\kappa(\leq 1)$を用いて保証する。次のようになる。

$$\tilde{Q}_{\mathrm{X}} \geq r_X \kappa\, \eta_X \mu \xi\left(\frac{r_X \kappa\, \eta_X \mu}{2}\right),$$

となり

$$\gamma = \frac{Q_{\mathrm{Z}} \tilde{Q}_{\mathrm{X}}}{Q_{\mathrm{X}} \tilde{Q}_{\mathrm{Z}}} \geq\ \kappa \frac{\xi\left(\frac{r_X \kappa\, \eta_X \mu}{2}\right)}{\xi(r_Z \eta_Z \mu)}.$$

$\xi(x)$は減少関数であるため、通常運転時の受動的基底選択確率の比が以下を満たせば$\gamma \geq \kappa$が保証される。

$$\frac{Q_{\mathrm{Z}}}{Q_{\mathrm{X}}} = \frac{r_Z \eta_Z}{r_X \eta_X} \geq \frac{1}{2}.$$

したがって、κ>0.285 で TOE が機能テストに合格した場合、TOE が侵入テストに不合格となる確率P_{fail} は無視できるほど小さいと結論づけることができる。

Revision history

Version	Date	Description
1.0	2025/05/13	First issue.

Review history

Summary of editing and reviewing processes

Core parts of the document were drafted by the QKD CC/PP Study Group under the MIC project.
Editing and reviewing of the document were conducted by
- QKD Implementation Security Study Group
- QKD Technical Review Committee
under the Quantum Forum (General Incorporated Association).
The drafts of the document were presented and discussed in ETSI ISG-QKD meetings.

Activity record of QKD Technical Review Committee

- 1st meeting (Nov. 19, 2024, 15:00~16:00)
  Discussion on review policy and schedule
- 1st round review on SD v0.43 (Nov. 19 - 29, 2024)

- 2nd meeting (Dec. 12, 2024, 18:00~19:00, jointly with QKD CC/PP SG)
  Discussion on the revised edition
- 2nd round review on SD v0.44 (Dec. 12- 23, 2024)

- 3rd meeting (Jan. 23, 2025, 18:00~20:40, jointly with QKD CC/PP SG)
  Discussion on the revised edition
- 3rd round review on SD v0.53 (Feb. 10- 17, 2025)

- 4th meeting (Feb. 20, 2025, 17:00~19:30, jointly with QKD CC/PP SG)
  Discussion on the revised edition
- 4th round review on SD v0.59 (Mar. 7- 21, 2025)

- 5th meeting (Mar. 21, 2025, 16:00~19:00, jointly with QKD CC/PP SG)
  Discussion on the revised edition
- 5th round review on SD v0.63r2 (Apr. 4- 9, 2025)

- 6th meeting (Apr. 10, 2025, 16:00~18:00, jointly with QKD CC/PP SG)
  Discussion on the revised edition
- 6th round review on SD v0.65r4 (Apr. 16- 21, 2025)

- 7th meeting (Apr. 17, 2025, 16:00~18:00, jointly with QKD CC/PP SG)
  Discussion on the revised edition

- 8th meeting (Apr. 24, 2025, 16:00~18:00, jointly with QKD CC/PP SG)
  Discussion on the revised edition

Discussion record in ETSI

- ISG-QKD#36f, Nov. 5, 2024
  Introduction on QKD module certification activities in Japan
- ISG-QKD#37, Dec. 2-4, 2024
  Discussion on SD v0.43
- ISG-QKD#37b, Jan. 7, 2025
  Discussion on SD v0.47
- ISG-QKD#37c, Feb. 4, 2025
  Discussion on SD v0.51
- ISG-QKD#37d, Mar. 4, 2025
  Discussion on SD v0.58
- ISG-QKD#37e, Apr. 1, 2025
  Discussion on SD v0.62
- ISG-QKD#37e, May. 6, 2025
  Discussion on SD v0.67

End of document