

ICS 35.030  
CCS L 80



**NATIONAL STANDARD OF THE  
PEOPLE'S REPUBLIC OF CHINA**

**GB/T 47679.2-2026**

---

**Cybersecurity technology - Security requirements, test and  
evaluation methods for quantum key distribution - Part 2: Test  
and evaluation methods**

网络安全技术 量子密钥分发的安全要求、测试和评估方法 第2部分：测试和评估  
方法

**(English Translation)**

**Issued on: May 25, 2026**

**Implemented on: December 1, 2026**

---

**Issued by: State Administration for Market Regulation**

## Table of Contents

|                                                                                            |    |
|--------------------------------------------------------------------------------------------|----|
| Preface                                                                                    |    |
| Introduction                                                                               |    |
| 1 Scope                                                                                    |    |
| 2 Normative References                                                                     |    |
| 3 Terms and Definitions                                                                    |    |
| 4 Abbreviations                                                                            | 3. |
| 5 Overview of QKD module evaluation methods                                                |    |
| 5.1 General Instructions                                                                   |    |
| 5.2 EM Range                                                                               |    |
| 5.3 Overview of Safety Functional Requirements Assessment Activities                       |    |
| 5.4 Overview of Security Assurance Requirements Assessment Activities                      |    |
| 6 EA for FTP_QKD                                                                           | 7. |
| 6.1 General Instructions                                                                   |    |
| 6.2 Testing Quantum State Transmission and Screening Procedures                            |    |
| 6.3 Testing other post-processors                                                          |    |
| 6.4 Test Parameter Calibration Procedure                                                   |    |
| 7 Evaluation of the quantum optics components of the transmitter module (EA 17)            |    |
| 7.1 General Notes                                                                          |    |
| 7.2 Test photon number distribution of the light pulse                                     |    |
| 7.3 Testing the average photon number and stability of optical pulses                      |    |
| 7.4 Testing the Independence of Light Pulse Intensity                                      |    |
| 7.5 Testing the accuracy of quantum state encoding                                         |    |
| 7.6 Testing the indistinguishability of encoded quantum states                             |    |
| 7.7 Testing the global phase distribution uniformity of the optical pulse                  |    |
| 7.8 Test the optical isolation of the transmitting module (32).                            |    |
| 7.9 Testing the sensitivity of the injected light detector in the transmitter module (34). |    |
| 7.10 Testing the robustness of the transmitter module to laser injection                   |    |
| 8 Evaluation of the quantum optics components of the receiver module (EA 39)               |    |
| 8.1 General Notes                                                                          |    |
| 8.2 Testing the consistency of receiver module detection efficiency                        |    |
| 8.3 Testing the leakage of reverse fluorescence information in the receiver module         |    |
| 8.4 Test the optical isolation of the receiver module (45).                                |    |

- 8.5 Testing the sensitivity of the receiver module's injected light detector.
- 8.6 Testing the robustness of the receiver module to blinding effects of strong light
- 8.7 Testing the compliance of single-photon detector dead time settings
- 8.8 Testing the detection efficiency time distribution of single-photon detectors
- 8.9 Testing the robustness of the receiver module to laser injection
- 8.10 Test the detection limit of the receiver module's zero-difference detector.
- 8.11 Testing Double-Counter Event Handling Compliance
- 9 Evaluation Parameter Calibration Procedure EA
  - 9.1 General Notes
  - 9.2 Test Detection Efficiency Mismatch Inducibility
  - 9.3 Testing the Correctness of Shot Noise Calibration
- 10 Supplemental activities to assess the security function requirements of traditional network components
  - 10.1 General Notes
  - 10.2 Overview of Assessment Activities for Safety Functional Requirements Related to FCS
  - 10.3 Overview of Assessment Activities for Other Safety Functional Requirements
- 11 Supplementary activities to security requirements
  - 11.1 General Notes
  - 11.2 APE Class. Supplementary Activities for Protective Profile Assessment
  - 11.3 ASE Category. Supplementary Activities to Security Target Assessment
  - 11.4 ADV Class. Developed Supplementary Activities
  - 11.5 AGD Category. Supplementary Activities to Guidance Documentation
  - 11.6 ATE Class. Supplementary Activities for Testing
  - 11.7 AVA Class. Supplementary Activities to Vulnerability Assessment
- 12 Compliance Statements
  - 12.1 General Notes
  - 12.2 Statement of Compliance with SFR Assessment Activities
  - 12.3 Compliance Statement Regarding SAR Assessment Activities
- Appendix A (Informative) Guidelines for Calculating Attack Potential in QKD Module Evaluation
- Appendix B (Informative) Example 79 of AVA Attack Potential Calculation Rating
- Appendix C (Informative) Threshold Set
- Appendix D (Informative) Assessment Activities and Known Attacks on Quantum Optical Devices and Parameter Calibration Procedures for Quantum Key Distribution Modules
- Correspondence between

## References

## Foreword

This document complies with the provisions of GB/T 1.1-2020 "Standardization Work Guidelines Part 1: Structure and Drafting Rules of Standardization Documents".

Drafting.

This document is Part 2 of GB/T 47679 "Security Requirements, Test and Evaluation Methods for Quantum Key Distribution in Network Security Technology".

GB/T 47679 has published the following parts.

---Part 1: Requirements;

---Part 2: Testing and Evaluation Methods.

This document is equivalent to ISO/IEC 23837-2:2023 "Security requirements, test and evaluation methods for quantum key distribution for information security".

Part 2: Evaluation and Testing Methods.

The following minimal editorial changes have been made to this document.

---To align with existing standards, the standard's name has been changed to "Security Requirements, Testing, and Evaluation for Quantum Key Distribution in Cybersecurity Technology".

Methods Part 2: Testing and Evaluation Methods;

---To align with existing standards, Chapter 1 includes additional information clarifying the scope of this document;

---The URLs for the ISO and IEC terminology databases have been removed;

---To improve the readability of standard documents, abbreviations such as ADV, AGD, APE, ASE, ATE, FSP, FTP, and ST are added.

Please note that some content in this document may involve patents. The issuing organization of this document assumes no responsibility for identifying patents.

This document was proposed and is under the jurisdiction of the National Cybersecurity Standardization Technical Committee (SAC/TC260).

## Introduction

GB/T 47679 "Security Requirements, Test and Evaluation Methods for Quantum Key Distribution in Network Security Technology" is based on GB/T 18336 (all parts).

Within the framework of (), this document establishes the security requirements, testing, and evaluation methods for quantum key distribution (QKD) modules. This document primarily specifies...

General safety assessment methods and corresponding assessment activities for QKD modules, including assessments of the relevant safety functions of QKD modules in GB/T 47679.1-2026.

Supplemental assessment activities for Security Assurance Requirements (SFR), and Security Assurance Requirements (SAR) for Assurance Levels (EAL) 1 to EAL5.

Supplementary assessment activities.

GB/T 47679 is proposed to consist of two parts.

---Part 1: Requirements. The aim is to establish a general framework for the security assessment of QKD modules and to provide a common basis for QKD modules.

Line SFR set.

---Part 2: Testing and Evaluation Methodology. The aim is to establish testing and evaluation methods for QKD security assessment, and to provide specific methods for...

The evaluation method for the QKD protocol, the quantum optical components in the QKD module, and the SFRs of traditional network components constituted by the test and evaluation system.

The assessment activities should be evaluated, and supplementary assessment activities should be provided to meet the security requirements of the corresponding assurance level QKD.

This document presents the QKD protocol implementation, as well as the testing and evaluation of quantum optics components in the QKD sender and receiver modules.

Activities. For SFRs specific to traditional network components, this document does not specify particular evaluation activities; it primarily refers to existing evaluation methods for network equipment.

This document also clarifies supplementary assessment activities for security assurance requirements and addresses the common vulnerability analysis in GB/T 30270-2024.

The methodology has been refined, covering guidelines for calculating attack potential.

The purpose of this document is to provide technical specifications for QKD manufacturers to improve the design and implementation security of QKD modules, and to guide evaluation methods.

This involves conducting testing and security assessments of QKD modules to reduce the risks associated with security function failures during QKD system operation.