ISO/IEC 23837-2:2023-09 (E)

Information security - Security requirements, test and evaluation methods for quantum key distribution - Part 2: Evaluation and testing methods

Contents

Page

Foreword ... **vi**

Introduction ... **vii**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Abbreviated terms ... **3**

5 Overview of the evaluation method for QKD modules ... **4**
- 5.1 General ... 4
- 5.2 Scope of the evaluation method ... 4
- 5.3 Overview of evaluation activities for SFRs ... 5
  - 5.3.1 General ... 5
  - 5.3.2 EAs for SFRs FTP_QKD.1 and FTP_QKD.2 ... 6
  - 5.3.3 EAs for SFRs on quantum optical components and parameter adjustment procedure(s) ... 6
  - 5.3.4 EAs for SFRs on conventional network components ... 7
  - 5.3.5 Thresholds and input parameters related to the evaluation activities ... 7
- 5.4 Overview of evaluation activities for SARs ... 8

6 EAs for the evaluation of FTP_QKD ... **8**
- 6.1 General ... 8
- 6.2 EA to test quantum state transmission and sifting procedures ... 10
  - 6.2.1 General aspects ... 10
  - 6.2.2 Test procedure ... 12
  - 6.2.3 Pass/fail criteria ... 14
- 6.3 EA to test other post-processing procedures ... 14
  - 6.3.1 General aspects ... 14
  - 6.3.2 Test procedure ... 16
  - 6.3.3 Pass/fail criteria ... 17
- 6.4 EA to test parameter adjustment procedure(s) ... 17
  - 6.4.1 General aspects ... 17
  - 6.4.2 Test procedure ... 19
  - 6.4.3 Pass/fail criteria ... 19

7 EAs for evaluating quantum optical components in the transmitter module ... **19**
- 7.1 General ... 19
- 7.2 EA to test the photon-number distribution of optical pulses ... 22
  - 7.2.1 General aspects ... 22
  - 7.2.2 Test procedure ... 24
  - 7.2.3 Pass/fail criteria ... 25
- 7.3 EA to test the mean photon number and stability of optical pulses ... 25
  - 7.3.1 General aspects ... 25
  - 7.3.2 Test procedure ... 26
  - 7.3.3 Pass/fail criteria ... 28
- 7.4 EA to test the independence of the intensities of optical pulses ... 28
  - 7.4.1 General aspects ... 28
  - 7.4.2 Test procedure ... 29
  - 7.4.3 Pass/fail criteria ... 30
- 7.5 EA to test the accuracy of state encoding ... 30
  - 7.5.1 General aspects ... 30

7.5.2 Test procedure 31
7.5.3 Pass/fail criteria 32
7.6 EA to test the indistinguishability of encoded states 32
7.6.1 General aspects 32
7.6.2 Test procedure 34
7.6.3 Pass/fail criteria 35
7.7 EA to test the uniform distribution of the global phase of optical pulses 36
7.7.1 General aspects 36
7.7.2 Test procedure 37
7.7.3 Pass/fail criteria 38
7.8 EA to test the degree of optical isolation of the TX module 38
7.8.1 General aspects 38
7.8.2 Test procedure 40
7.8.3 Pass/fail criteria 40
7.9 EA to test the sensitivity of the injected light monitor in the TX module 40
7.9.1 General aspects 40
7.9.2 Test procedure 41
7.9.3 Pass/fail criteria 42
7.10 EA to test the robustness of the TX module against laser injection 42
7.10.1 General aspects 42
7.10.2 Test procedure 44
7.10.3 Pass/fail criteria 46

8 EAs for the evaluation of quantum optical components in the receiver module 47
8.1 General 47
8.2 EA to test the consistency of detection probability in the RX module 49
8.2.1 General aspects 49
8.2.2 Test procedure 51
8.2.3 Pass/fail criteria 51
8.3 EA to test information leakage of back-flashes from the RX module 52
8.3.1 General aspects 52
8.3.2 Test procedure 53
8.3.3 Pass/fail criteria 54
8.4 EA to test the degree of optical isolation of the RX module 54
8.4.1 General aspects 54
8.4.2 Test procedure 55
8.4.3 Pass/fail criteria 55
8.5 EA to test the sensitivity of the injected light monitor in the RX module 56
8.5.1 General aspects 56
8.5.2 Test procedure 57
8.5.3 Pass/fail criteria 57
8.6 EA to test the robustness of the RX module against bright light blinding 58
8.6.1 General aspects 58
8.6.2 Test procedure 59
8.6.3 Pass/fail criteria 60
8.7 EA to test the appropriateness of dead time settings of SPDs 60
8.7.1 General aspect 60
8.7.2 Test procedure 61
8.7.3 Pass/fail criteria 62
8.8 EA to test the temporal profile of the detection efficiency for SPDs 62
8.8.1 General aspects 62
8.8.2 Test procedure 63
8.8.3 Pass/fail criteria 63
8.9 EA to test the robustness of the RX module against laser injection 64
8.9.1 General aspects 64
8.9.2 Test procedure 65
8.9.3 Pass/fail criteria 66
8.10 EA to test the detection limits of homodyne detectors in the RX module 67
8.10.1 General aspects 67
8.10.2 Test procedure 67
8.10.3 Pass/fail criteria 68
8.11 EA to test the appropriateness of double-click event handling 68
8.11.1 General aspects 68
8.11.2 Test procedure 69

        8.11.3 Pass/fail criteria ... 69

9 EAs for the evaluation of parameter adjustment procedure(s) ... 69

    9.1 General ... 69
    9.2 EA to test the inducibility of detection probability mismatch ... 70
        9.2.1 General aspects ... 70
        9.2.2 Test procedure ... 73
        9.2.3 Pass/fail criteria ... 74
    9.3 EA to test the correctness of shot noise alignment ... 74
        9.3.1 General aspects ... 74
        9.3.2 Test procedure ... 75
        9.3.3 Pass/fail criteria ... 77

10 Supplementary activities for the evaluation of SFRs on conventional network components ... 77

    10.1 General ... 77
    10.2 Evaluation activities for FCS related SFRs overview ... 78
    10.3 Evaluation activities for other SFRs overview ... 78

11 Supplementary activities for SARs ... 78

    11.1 General ... 78
    11.2 Supplementary activities for Class APE: Protection Profile evaluation ... 78
    11.3 Supplementary activities for Class ASE: Security Target evaluation ... 80
    11.4 Supplementary activities for Class ADV: Development ... 80
        11.4.1 Supplementary activities for ADV_ARC ... 80
        11.4.2 Supplementary activities for ADV_FSP ... 81
    11.5 Supplementary activities for Class AGD: Guidance documents ... 82
        11.5.1 Supplementary activities for AGD_OPE ... 82
        11.5.2 Supplementary activities for AGD_PRE ... 83
    11.6 Supplementary activities for Class ATE: Test ... 83
        11.6.1 Supplementary activities for ATE_FUN ... 83
        11.6.2 Supplementary activities for ATE_IND ... 84
    11.7 Supplementary activities for Class AVA: Vulnerability assessment ... 85

12 Conformance statement ... 88

    12.1 General ... 88
    12.2 Conformance statement specific to evaluation activities for SFRs ... 88
    12.3 Conformance statement specific to EAs for SARs ... 89

Annex A (informative) **Guidance on the calculation of attack potential for the evaluation of QKD modules ... 90**

Annex B (informative) **Rating examples for AVA attack potential computation ... 97**

Annex C (informative) **Thresholds collection ... 100**

Annex D (informative) **Correspondence between EAs and known attacks to quantum optical components and parameter adjustment procedure(s) of QKD modules ... 104**

Bibliography ... 106