ISO/IEC 17825:2024-01 (E)

Information technology - Security techniques - Testing methods for the mitigation of non-invasive attack classes against cryptographic modules

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

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

4 Symbols and abbreviated terms ... **3**

5 Document organization ... **4**

6 Non-invasive attack methods ... **4**

7 Non-invasive attack test methods ... **7**
7.1 General ... 7
7.2 Test strategy ... 7
7.3 Side-channel analysis workflow ... 8
7.3.1 Core test flow ... 8
7.3.2 Side-channel resistance test framework ... 8
7.3.3 Required vendor information ... 9
7.3.4 TA leakage analysis ... 10
7.3.5 SPA/SEMA leakage analysis ... 11
7.3.6 DPA/DEMA leakage analysis ... 12

8 Side-channel analysis of symmetric-key cryptosystems ... **13**
8.1 General ... 13
8.2 Timing attacks ... 13
8.3 SPA/SEMA ... 13
8.3.1 Attacks on key derivation process ... 13
8.3.2 Side-channel collision attacks ... 14
8.4 DPA/DEMA ... 14

9 ASCA on asymmetric cryptography ... **16**
9.1 General ... 16
9.2 Detailed side-channel resistance test framework ... 17
9.3 Timing attacks ... 18
9.3.1 General ... 18
9.3.2 Standard timing analysis ... 18
9.3.3 Micro-architectural timing analysis ... 19
9.4 SPA/SEMA ... 19
9.5 DPA/DEMA ... 19

Annex A (normative) **Non-invasive attack mitigation pass/fail test metrics** ... **21**

Annex B (informative) **Requirements for measurement apparatus** ... **24**

Annex C (informative) **Associated security functions** ... **25**

Annex D (informative) **Emerging attacks** ... **27**

Annex E (informative) **Quality criteria for measurement setups** ... **30**

Annex F (informative) **Chosen-input method to accelerate leakage analysis** ... **32**

Annex G (informative) **Reasons that a side-channel is assessed as not measurable** ... **33**

Annex H (informative) **Information about leakage location in relation to algorithm time** ... **34**

Bibliography ... **35**