ISO/IEC 20085-1:2019-10 (E)

IT Security techniques - T est tool requirements and test tool calibration methods for use in testing non-i nvasive attack mitigation techniques in cryptographic modules - Part 1: Test too ls and techniques

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Symbols and abbreviated terms 3

5 Test tools 3
5.1 General 3
5.2 Types of side-channels 4
5.2.1 General 4
5.2.2 Power consumption 4
5.2.3 Electromagnetic emissions 4
5.2.4 Computation time 4
5.3 Categorization of test tool 4
5.4 Test tool components 5
5.4.1 General 5
5.4.2 Measurement tool 5
5.4.3 Analysis tool 7
5.4.4 Functional items of test tools components 7

6 Test techniques and associated approaches 8
6.1 Operation 8
6.2 Interaction between the measurement tool and the IUT 9
6.3 Interaction between the analysis tool and the IUT 9
6.4 Interaction between the analysis tool and the measurement tool 9

Annex A (informative) Selection of test methods and approaches 10

Annex B (informative) Example of measurement tool 15

Annex C (informative) Data exchange and storing technologies 17

Bibliography 18