

# ISO/IEC 20085-2:2020-03 (E)

## IT Security techniques - Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules - Part 2: Test calibration methods and apparatus

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	1
4	Abbreviated terms .....	2
5	Test tools .....	2
5.1	Tools and analysis .....	2
5.2	Determining the test result .....	2
5.3	Measurement tool .....	2
5.4	Analysis tool .....	2
6	Calibration methods .....	3
6.1	Aspects .....	3
6.2	Introduction to calibration procedure .....	3
6.2.1	General knowledge of calibration procedure .....	3
6.2.2	Accuracy of test tools .....	3
6.2.3	Measurement tool .....	4
6.2.4	Calibration principle .....	4
6.3	Calibration procedure .....	4
6.3.1	General .....	4
6.3.2	Point of measurement .....	5
6.3.3	Parameter adjustment .....	5
6.4	Calibration metrics .....	5
7	Artefact .....	6
7.1	General .....	6
7.2	Side-channel analysis .....	6
7.3	Open target .....	6
7.3.1	General .....	6
7.3.2	General specification .....	6
7.3.3	Example specification .....	6
7.4	Closed target .....	6
Annex A (informative)	Cryptographic algorithms and calibration metrics .....	7
Annex B (informative)	Countermeasures to tune the security strength .....	9
Annex C (informative)	An example artefact implementation -- A hardware security module emulated with an FPGA .....	11
Annex D (informative)	An example artefact implementation -- A microcontroller .....	13
Annex E (informative)	An example artefact implementation -- Signal generator .....	15
Bibliography .....		16