

# ISO/IEC 17825:2016-01 (E)

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

---

<b>Contents</b>		<b>Page</b>
Foreword .....		v
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	1
4	Symbols and abbreviated terms .....	4
5	Document organization .....	4
6	Non-invasive attack methods .....	4
7	Associated Security Functions .....	7
8	Non-invasive Attack Test Methods .....	9
8.1	Introduction .....	9
8.2	Test Strategy .....	9
8.3	Side-Channel Analysis Workflow .....	9
8.3.1	Core Test Flow .....	9
8.3.2	Side-Channel Resistance Test Framework .....	10
8.3.3	Required Vendor Information .....	11
8.3.4	TA Leakage Analysis .....	12
8.3.5	SPA/SEMA Leakage Analysis .....	13
8.3.6	DPA/DEMA Leakage Analysis .....	14
9	Side-Channel Analysis of Symmetric-Key Cryptosystems .....	15
9.1	Introduction .....	15
9.2	Timing Attacks .....	15
9.3	SPA/SEMA .....	15
9.3.1	Attacks on Key Derivation Process .....	15
9.3.2	Collision Attacks .....	16
9.4	DPA/DEMA .....	16
9.4.1	Introduction .....	16
9.4.2	Test Vectors .....	18
9.4.3	Detailed Procedure .....	19
10	ASCA on Asymmetric Cryptography .....	25
10.1	Introduction .....	25
10.2	Detailed Side-Channel Resistance Test Framework .....	27
10.3	Timing Attacks .....	28
10.3.1	Introduction .....	28
10.3.2	Standard Timing Analysis .....	28
10.3.3	Micro-Architectural Timing Analysis .....	29
10.4	SPA/SEMA .....	29
10.4.1	Introduction .....	29
10.4.2	Standard SPA/SEMA .....	29
10.4.3	Markov SPA/SEMA .....	30
10.5	DPA/DEMA .....	30
10.5.1	Introduction .....	30

10.5.2	Standard DPA/DEMA .....	30
10.5.3	Address-Bit DPA/DEMA .....	32
11	Non-invasive attack mitigation pass/fail test metrics .....	33
11.1	Introduction .....	33
11.2	Security Level 3 .....	34
11.2.1	Time Limit .....	34
11.2.2	SPA and SEMA .....	34
11.2.3	DPA and DEMA .....	34
11.2.4	Timing Analysis .....	34
11.2.5	Pre-processing conditions in differential analysis .....	34
11.2.6	Pass / Fail condition .....	34
11.3	Security Level 4 .....	35
11.3.1	Time Limit .....	35
11.3.2	SPA and SEMA .....	35
11.3.3	DPA and DEMA .....	35
11.3.4	Timing Analysis .....	35
11.3.5	Pre-processing conditions in differential analysis .....	35
11.3.6	Pass / Fail condition .....	36
	Annex A (normative) Requirements for measurement apparatus .....	37
	Annex B (informative) Emerging attacks .....	38
	Annex C (informative) Quality criteria for measurement setups .....	40
	Annex D (informative) Chosen-input method to accelerate leakage analysis .....	42
	Bibliography .....	43