

# 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
<b>1 Scope.....</b>	<b>1</b>
<b>2 Normative references.....</b>	<b>1</b>
<b>3 Terms and definitions.....</b>	<b>1</b>
<b>4 Symbols and abbreviated terms.....</b>	<b>3</b>
<b>5 Document organization.....</b>	<b>4</b>
<b>6 Non-invasive attack methods.....</b>	<b>4</b>
<b>7 Non-invasive attack test methods.....</b>	<b>7</b>
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
<b>8 Side-channel analysis of symmetric-key cryptosystems.....</b>	<b>13</b>
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
<b>9 ASCA on asymmetric cryptography.....</b>	<b>16</b>
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
<b>Annex A (normative) Non-invasive attack mitigation pass/fail test metrics.....</b>	<b>21</b>
<b>Annex B (informative) Requirements for measurement apparatus.....</b>	<b>24</b>
<b>Annex C (informative) Associated security functions.....</b>	<b>25</b>
<b>Annex D (informative) Emerging attacks.....</b>	<b>27</b>
<b>Annex E (informative) Quality criteria for measurement setups.....</b>	<b>30</b>
<b>Annex F (informative) Chosen-input method to accelerate leakage analysis.....</b>	<b>32</b>
<b>Annex G (informative) Reasons that a side-channel is assessed as not measurable.....</b>	<b>33</b>
<b>Annex H (informative) Information about leakage location in relation to algorithm time.....</b>	<b>34</b>
<b>Bibliography.....</b>	<b>35</b>