This is a preview - click here to buy the full publication

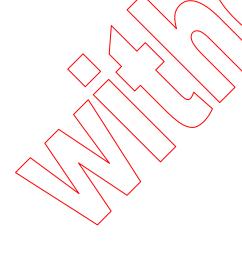
# INTERNATIONAL STANDARD

# 17825

First edition 2016-01-15

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

Technologie de l'information — Techniques de sécurité — Methodes de test pour la protection contre les attaques non intrusives des modules cryptographiques









### **COPYRIGHT PROTECTED DOCUMENT**

## $\, @ \,$ ISO/IEC 2016, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office Ch. de Blandonnet 8 • CP 401 CH-1214 Vernier, Geneva, Switzerland Tel. +41 22 749 01 11 Fax +41 22 749 09 47 copyright@iso.org www.iso.org

Coı	Contents			
Forewordv				
1	Scop	e	1	
2	Norn	native references	1	
3		ns and definitions		
4		ools and abbreviated terms		
5	-	iment organization		
6		invasive attack methods		
7				
	Associated Security Functions Non-invasive Attack Test Methods			
8	8.1 8.2 8.3	Introduction Test Strategy Side-Channel Analysis Workflow 8.3.1 Core Test Flow 8.3.2 Side-Channel Resistance Test Framework 8.3.3 Required Vendor Information 8.3.4 TA Leakage Analysis 8.3.5 SPA/SEMA Leakage Analysis 8.3.6 DPA/DEMA Leakage Analysis	99 99 10 11 12 13 13 14	
9	9.1 9.2 9.3	Channel Analysis of Symmetric-Key Cryptosystems Introduction Timing Attacks SPA/SEMA 9.3.1 Attacks on Key Derivation Process 9.3.2 Collision Attacks DPA/DEMA	15 15 15 15	
10		9.4.1 Introduction 9.4.2 Test Vectors 9.4.3 Detailed Procedure  on Asymmetric Cryptography	16 18 19	
10		Introduction Introduction	25	
	10.2	Detailed Side-Channel Resistance Test Framework		
	10.3	Timing Attacks		
		10.3.2 Standard Timing Analysis		
	10.4	10.3.3 Micro-Architectural Timing Analysis SPA/SEMA 10.4.1 Introduction 10.4.2 Standard SPA/SEMA 10.4.3 Markov SPA/SEMA	29 29 29	
	10.5	DPA/DEMA 10.5.1 Introduction 10.5.2 Standard DPA/DEMA 10.5.3 Address-Bit DPA/DEMA	30 30 30	
11	Non-invasive attack mitigation pass/fail test metrics			
	11.1 11.2	Introduction Security Level 3		
		11.2.1 Time Limit	34	
		11.2.2 SPA and SEMA		
		11.2.3 DPA and DEMA 11.2.4 Timing Analysis		

# ISO/IEC 17825:2016(E)

	11.2.5 Pre-processing conditions in differential analysis	
	11.2.6 Pass / Fail condition	
11.3	Security Level 4	
	11.3.1 Time Limit	
	11.3.2 SPA and SEMA	
	11.3.4 Timing Analysis	
	11.3.5 Pre-processing conditions in differential analysis	
	11.3.6 Pass / Fail condition	
Annex A (no	rmative) Requirements for measurement apparatus	37
Annex B (inf	ormative) Emerging attacks	38
Annex C (info	ormative) Quality criteria for measurement setups	40
	Formative) Chosen-input method to accelerate leakage analysis.	\
Bibliography	v	43

#### Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC | TC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see <a href="https://www.iso.org/directives">www.iso.org/directives</a>).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see <a href="https://www.iso.org/patents">www.iso.org/patents</a>).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.



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

# 1 Scope

This International Standard specifies the non-invasive attack mitigation test metrics for determining conformance to the requirements specified in ISO/IEC 19790 for Security Levels 3 and 4. The test metrics are associated with the security functions specified in ISO/IEC 19790. Testing will be conducted at the defined boundary of the cryptographic module and I/O available at its defined boundary.

The test methods used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790 and the test metrics specified in this International Standard for each of the associated security functions specified in ISO/IEC 19790 are specified in ISO/IEC 24759. The test approach employed in this International Standard is an efficient "push-button" approach: the tests are technically sound, repeatable and have moderate costs.

## 2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 19790, Information technology — Security techniques — Security requirements for cryptographic modules

ISO/IEC 24759, Information technology — Security techniques — Test requirements for cryptographic modules