

American National Standard

INCITS/ISO/IEC 17825:2016 (2018)

(ISO/IEC 17825:2016, IDT)

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

Developed by



Where IT all begins



INCITS/ISO/IEC 17825:2016 (2018)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

Adopted by INCITS (InterNational Committee for Information Technology Standards) as an American National Standard.

Date of ANSI Approval: 9/11/2018

Published by American National Standards Institute,
25 West 43rd Street, New York, New York 10036

Copyright 2018 by Information Technology Industry Council
(ITI). All rights reserved.

These materials are subject to copyright claims of International Standardization Organization (ISO), International Electrotechnical Commission (IEC), American National Standards Institute (ANSI), and Information Technology Industry Council (ITI). Not for resale. No part of this publication may be reproduced in any form, including an electronic retrieval system, without the prior written permission of ITI. All requests pertaining to this standard should be submitted to ITI, 1101 K Street NW, Suite 610, Washington DC 20005.

Printed in the United States of America

First edition
2016-01-15

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

Techonologie 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

This is a preview of "INCITS/ISO/IEC 17825...". Click here to purchase the full version from the ANSI store.

Contents

	Page
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

This is a preview of "INCITS/ISO/IEC 17825...". Click [here](#) to purchase the full version from the ANSI store.

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

This is a preview of "INCITS/ISO/IEC 17825...". Click here to purchase the full version from the ANSI store.

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 JTC 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 www.iso.org/directives).

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 www.iso.org/patents).

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*.