INTERNATIONAL STANDARD

ISO/IEC 20085-2

First edition
2020-03

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

Techniques de sécurité IT — Exigences de l'outil de test et méthodes d'étalonnage de l'outil de test utilisées pour tester les techniques d'atténuation des attaques non invasives dans les modules cryptographiques —

Partie 2: Méthodes et appareillage d'étalonnage et d'essai

Reference number
ISO/IEC 20085-2:2020(E)

© ISO/IEC 2020



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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**

© ISO/IEC 2020 – All rights reserved

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.

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) or the IEC list of patent declarations received (see http://patents.iec.ch).

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 20085 series can be found on the ISO website.

© ISO/IEC 2020 – All rights reserved

Introduction

Cryptographic modules provide cryptographic services and protect critical security parameters. Protection of critical security parameters can either be logical, physical, or both. Information such as knowledge of critical security parameters can leak out of the cryptographic module during operation, if the module is not designed to mitigate such leakage. Without mitigation, a malevolent attacker can record available side-channel leakage. This leakage is a physical quantity related to the critical security parameters and can be analysed in a manner to extract information about those parameters. Such analysis is passive, in that it simply collects the side-channel leakage measurements which can be freely acquired with an apparatus. Notice that the measurement tool can, as well, be adaptively controlled. This kind of extraction and analysis is referred to as non-invasive. Techniques that allow the extraction of critical security parameters out of this non-invasive leakage is termed an *attack* on the module.

Non-invasive attack testing is a method to determine whether the leakage of a cryptographic module can be exploited to extract critical security parameters. A non-invasive attack test tool returns a pass status if the cryptographic module leakage is determined to be of a minimal amount which may prevent disclosure of critical security parameters. Otherwise, it returns a fail status.

This document focuses on the calibration of the side-channel measurement tool. This calibration process enables two measurement tools to record measurements equally usable in terms of side channel analysis. Calibration is presented as the combination of two techniques:

a) definition of a method for calibration;

b) requirement of a reference cryptographic module (called an artefact) to define a clear threshold between test results, in terms of fail or pass.

Both aspects are covered in this document.

© ISO/IEC 2020 – All rights reserved

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

1 Scope

This document specifies the test calibration methods and apparatus used when calibrating test tools for cryptographic modules under ISO/IEC 19790 and ISO/IEC 24759 against the test metrics defined in ISO/IEC 17825 for mitigation of non-invasive attack classes.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 17825, *Information technology — Security techniques — Testing methods for the mitigation of non-invasive attack classes against cryptographic modules*

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

ISO/IEC 20085-1, *IT Security techniques — Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 1: Test tools and techniques*

3 Terms and definitions

For the purposes of this document, the terms, definitions given in ISO/IEC 19790, ISO/IEC 17825, ISO/IEC 20085-1, and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
artefact
signal source which is representative of a leaking device for use when conducting *calibration* (3.2)

Note 1 to entry: Its purpose is to generate information from sensitive data. It mimics the leakage from an actual cryptographic module when operated.

3.2
calibration
process of setting threshold to adequate values, such that the border between pass and fail can be reproduced identically between different non-invasive test tools

© ISO/IEC 2020 – All rights reserved

3.3
countermeasure
design method aiming at reducing the information leakage

3.4
security strength
number of traces to detect a leakage using ISO/IEC 17825 metrics

4 Abbreviated terms

A/D Analog/Digital

AES Advanced Encryption Standard[14]

RSA Rivest–Shamir–Adleman[15]

5 Test tools

5.1 Tools and analysis

A test tool for non-invasive attack mitigation for cryptographic modules consists of collecting side-channel information in a non-invasive manner, reprocessing it (e.g. aligning and filtering), and applying corresponding analysis methods to determine whether the target module leaks critical information. A test tool, conforming to ISO/IEC 20085-1, consists of a data measurement tool and an analysis tool. A single test tool can test different analysis types of attack including power analysis, electromagnetic analysis, and timing analysis as shown in ISO/IEC 17825. The measurement tool contains a probe that converts a particular physical quantity, such as electric current, into an electric voltage level at a certain conversion ratio (or a more complex relationship in case the relationship is not linear), where the measurement tool captures the voltage level with an A/D converter and stores the digital data into internal storage at a specified capturing rate. A triggering mechanism is necessary to determine the capture timings. Triggering can require a dedicated probe connected to a specified part of the IUT in order to provide accurate capture timings. The analysis tool is a computer that controls the test process as well as carries out analysis computations.

5.2 Determining the test result

The specification and operation of the test tool shall meet the requirements described in ISO/IEC 20085-1. The purpose of the test tool is to determine whether the amount of leaked information as the result of the side-channel analysis is below or above a given threshold M as specified in ISO/IEC 17825.

5.3 Measurement tool

The measurement tool in the non-invasive attack test can have some variations in its physical characteristics that can influence the test results. If two different test tools use the same analysis tool and, thus, the same test method and use different components in their measurement tools, the test results can be different. The calibration is conducted to compensate for this difference, which is attributed to the measurement tools.

5.4 Analysis tool

The analysis tool in the non-invasive attack test controls the measurement process and conducts the data-processing. These can be implemented deterministically, i.e. without the influence of any variance. There can be differences in the numeric precisions of computation, or the analysis algorithms adopted. Therefore, the tool calibration covers the complete test tool, including the measurement tool and analysis tool.

© ISO/IEC 2020 – All rights reserved