INTERNATIONAL STANDARD

**ISO/IEC 20085-1**

First edition
2019-10

# 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

*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 1: Outils et techniques de test*



Reference number
ISO/IEC 20085-1:2019(E)

**COPYRIGHT PROTECTED DOCUMENT**



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 Symbols and abbreviated terms** ... **3**
**5 Test tools** ... **3**
5.1 General ... 3
5.2 Types of side-channels ... 4
5.2.1 General ... 4
5.2.2 Power consumption ... 4
5.2.3 Electromagnetic emissions ... 4
5.2.4 Computation time ... 4
5.3 Categorization of test tool ... 4
5.4 Test tool components ... 5
5.4.1 General ... 5
5.4.2 Measurement tool ... 5
5.4.3 Analysis tool ... 7
5.4.4 Functional items of test tools components ... 7
**6 Test techniques and associated approaches** ... **8**
6.1 Operation ... 8
6.2 Interaction between the measurement tool and the IUT ... 9
6.3 Interaction between the analysis tool and the IUT ... 9
6.4 Interaction between the analysis tool and the measurement tool ... 9
**Annex A** (informative) **Selection of test methods and approaches** ... **10**
**Annex B** (informative) **Example of measurement tool** ... **15**
**Annex C** (informative) **Data exchange and storing technologies** ... **17**
**Bibliography** ... **18**

# 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.

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.

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.



 

# Introduction

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

This document focuses on the measurement and analysis of side-channel information. Side-channel non-invasive test tools can be automated to collect such leakage. To characterize the quality of the test tools, metrics are needed, such as signal-to-noise ratio (S/N) (described in ISO/IEC 20085-2). ISO/IEC 20085 (all parts) addresses the measurement and analysis techniques. Those are automated in a test tool. The functionality and the operation of a test tool are described in ISO/IEC 20085 (all parts).

# 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



## 1 Scope

This document provides specifications for non-invasive attack test tools and provides information about how to operate such tools. The purpose of the test tools is the collection of signals (i.e. side-channel leakage) and their analysis as a non-invasive attack on a cryptographic module implementation under test (IUT).

## 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 19790:2012, *Information technology — Security techniques — Security requirements for cryptographic modules*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given ISO/IEC 19790 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**
**advanced side-channel analysis**
**ASCA**
advanced exploitation of the fact that the instantaneous side-channels emitted by a cryptographic device depends on the data it processes and on the operation it performs to retrieve secret parameters

Note 1 to entry: Not to be confused with algebraic side-channel analysis (SCA).

Note 2 to entry: The adjective “advanced”, opposed to “simple”, qualifies side-channel analyses which require multiple side-channel measurements (see 6.2).

[SOURCE: ISO/IEC 17825:2016, 3.1, modified — Notes to entry have been added.]

**3.2**
**analysis tool**
test tool component with the ability to control the measurement process, read the recorded measurements, perform post-processing of the recorded measurements, and identify any valid attacks