

---

---

**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*



**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

ISO/IEC 20085-2:2020  
<https://standards.iteh.ai/catalog/standards/sist/eb7b8ba7-a106-4374-83d4-1bbbaa71d2a7/iso-iec-20085-2-2020>



**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](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# 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 Abbreviated terms.....</b>	<b>2</b>
<b>5 Test tools.....</b>	<b>2</b>
5.1 Tools and analysis.....	2
5.2 Determining the test result.....	2
5.3 Measurement tool.....	2
5.4 Analysis tool.....	2
<b>6 Calibration methods.....</b>	<b>3</b>
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
<b>7 Artefact.....</b>	<b>6</b>
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
<b>Annex A (informative) Cryptographic algorithms and calibration metrics.....</b>	<b>7</b>
<b>Annex B (informative) Countermeasures to tune the security strength.....</b>	<b>9</b>
<b>Annex C (informative) An example artefact implementation — A hardware security module emulated with an FPGA.....</b>	<b>11</b>
<b>Annex D (informative) An example artefact implementation — A microcontroller.....</b>	<b>13</b>
<b>Annex E (informative) An example artefact implementation — Signal generator.....</b>	<b>15</b>
<b>Bibliography.....</b>	<b>16</b>

## 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](http://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](http://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](http://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](http://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.

## 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 20085-2:2020](https://standards.iteh.ai/catalog/standards/sist/eb7b8ba7-a106-4374-83d4-1bbbaa71d2a7/iso-iec-20085-2-2020)

<https://standards.iteh.ai/catalog/standards/sist/eb7b8ba7-a106-4374-83d4-1bbbaa71d2a7/iso-iec-20085-2-2020>

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

ISO/IEC 2085-2:2020

<https://standards.iteh.ai/catalog/standards/sist/eb7b8ba7-a106-4374-83d4-1bbbaa71d2a7/iso-iec-2085-2-2020>

# 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

**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<sup>[14]</sup>
- RSA Rivest–Shamir–Adleman<sup>[15]</sup>

**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.



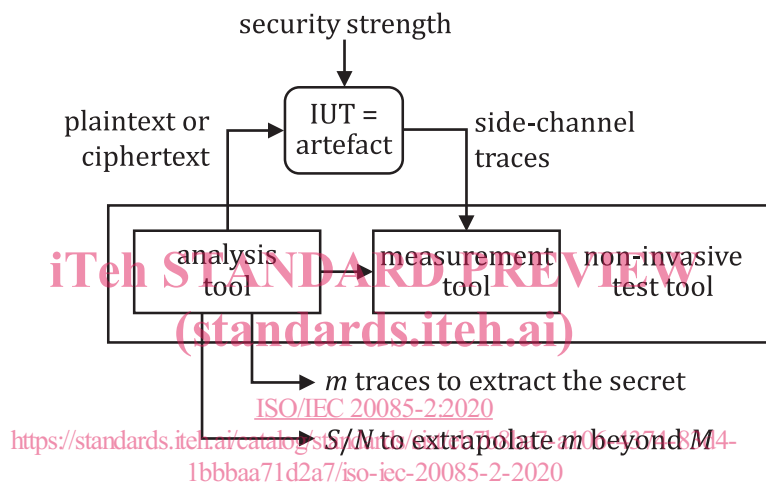
## 6 Calibration methods

### 6.1 Aspects

This clause discusses calibration methods.

The importance of calibration is to avoid the situation where an IUT is considered secure but in actual operation it is not due to the insufficient quality of the measurement tools. Such a situation would be detrimental to the trust in non-invasive attack evaluation and test methods. Calibration is a process related to the analysed cryptographic algorithm and IUT, its countermeasures (if any), the test equipment, and thereby provide mutual comparison and traceability.

The relationship between the calibration method and non-invasive test tool is depicted in [Figure 1](#). The constant  $M$  is the threshold in terms of number of measurements to extract critical security parameters (e.g. a secret key), according to ISO/IEC 17825, and  $m$  is the number of traces required to extract critical security parameters of the IUT.



**Figure 1 — Block diagram illustrating the relationship between calibration method and non-invasive test tool**

### 6.2 Introduction to calibration procedure

#### 6.2.1 General knowledge of calibration procedure

The non-invasive attack test tool calibration method specified in this clause is to enable different non-invasive test tools acquired from different sources to have a uniform test quality and, thus, the same test results. The calibration method shall be implemented by using two elements: the target test tool to be calibrated and the target IUT, which is also referred to as a test target apparatus or an artefact.

**NOTE** This document does not preclude from using multiple artefacts. A module (Device Under Test) passes or fails when tested by a test tool, calibrated according to one artefact. If multiple artefacts are used, they behave identically.

Such an artefact is designed to perform a certain mitigation level against particular non-invasive attacks. Tool developers may develop their own tools at the uniform quality achieved by calibrating their tools with a uniformly adjusted artefact.

#### 6.2.2 Accuracy of test tools

Each part of the test tool shall provide appropriate accuracies that meet the requirements specified in this document. These accuracies have some intrinsic connection; for example, the changes in sampling rate or the amount of jitter in the trigger affects the signal-to-noise ratio ( $S/N$ ) in a similar manner to additional noise in the measurement circuitry. Sampling clocks which are synchronized to the IUT clock

can result in a considerably better  $S/N$  compared to unsynchronized sampling clocks<sup>[1]</sup>. Unsynchronized sampling clocks require careful consideration especially if a calibration artefact provides a clock for the sampling device to synchronize, but the IUT does not.

The degree of precision is impacted by:

- quantization level (the number of bits that the A/D converter outputs);
- sampling rate (the frequency of data capturing), and source of sampling clock (synchronous to IUT clock or asynchronous);
- frequency bandwidth.

The degree of accuracy is impacted by:

- error in the voltage level (including the converted figure from the electric-current);
- error in timing;
- value of the  $S/N$  (estimated as per section 5.1 of Reference [16]).

### 6.2.3 Measurement tool

The measurement tool is an active device, which converts some physical quantity (time, power, electromagnetic radiation, etc.) into an electric quantity (e.g. voltage). It is characterized by its effect on the signal: ideally, it has little distortion, high bandwidth, and low noise figure (i.e. it does not reduce the  $S/N$  in a small proportion).

### 6.2.4 Calibration principle

Calibration of a non-invasive attack test tool is carried out to check whether the tool determines the test result of an IUT correctly at the given Security Level as prescribed in ISO/IEC 17825. Adjustments of the internal parameters of the tool can be necessary so that the tool correctly determines the test result.

Calibration can be used to achieve two goals.

Goal 1: To check whether

- a) an IUT which is built to pass, shall pass; and
- b) an IUT which is built to fail, shall fail.

Goal 2: To enable comparative tests with different test tools

A calibration process shall use a known target artefact whose behaviour and degree of mitigation against the subject attack methods are predetermined. The test tool to be calibrated shall be operated and adjusted in accordance with the calibration procedure so it shows test results within the predetermined range of the degree of mitigation against the target artefact. Thus, a single calibration procedure deals with two different degrees of mitigation that can be provided with a single artefact with a variable mitigation capability, or two different artefacts with slightly different degrees of mitigation that define the acceptable range.

## 6.3 Calibration procedure

### 6.3.1 General

Calibration procedures shall be performed using defined known types of artefacts. The calibration shall follow the test methods specified in ISO/IEC 17825 and ISO/IEC 20085-1 by testing the given artefact as an IUT. The calibration operator can adjust the test tool parameters by the specified procedures if necessary, so that the tool indicates the correct test results with regards to the defined mitigation level of the artefact.

A calibration process shall repeat the test procedure twice as specified in ISO/IEC 20085-1 for the subject Security Level by slightly changing the test parameters. The first test procedure shall repeat cryptographic operations as needed and the test tool shall gather the necessary information, shall analyse the data, and shall determine whether the target artefact passes or fails the test. The second test shall be performed with a little higher or lower test parameter and indicates the test result likewise.

If the test tool shows that its determination criteria is lower (tends to indicate passes, or overlooks the leakage) than a specified threshold, the calibration procedure of the test tool shall terminate indicating a failure of calibration. If the determination is higher (tends to indicate fails), the test tool conditioning parameters shall be adjusted accordingly.

The process is given in Algorithm 1 below.

Let  $M$  be the threshold trace number upon which an attack is termed successful according to ISO/IEC 17825, that is  $M = 10\ 000$  (Security Level 3) or  $M = 100\ 000$  (Security Level 4).

Algorithm 1: Calibration process.

```

1.   Input: test tool
2.   Output: accept or reject
3.   {
4.     The security strength is incrementally increased before the
       threshold is reached;
5.     Get the number of traces  $m0$  to detect a leakage;
6.     The security strength is incrementally decreased before the
       threshold is reached;
7.     Get the number of traces  $m1$  to recover the secret concealed
       by the artefact;
8.     if  $m0 < M$  and  $m1 > M$ :
9.       return accept;
10.    else
11.      return reject;
12.  }
```

The “accept” return value indicates that the non-invasive test tool is calibrated, whereas the “reject” return value indicates on the contrary that the non-invasive test tool is not calibrated.

The calibration illustrated in the flow chart of Algorithm 1 may be used repeatedly, until the non-invasive test tool is calibrated.

### 6.3.2 Point of measurement

If probes are used, whether electrical contacts or EM probes, they shall be placed on the specified points on the IUT as described in ISO/IEC 17825 and ISO/IEC 20085-1.

### 6.3.3 Parameter adjustment

Necessary adjustments may be conducted to maximize the  $S/N$  of the measurements.

## 6.4 Calibration metrics

Calibration metrics for particular cryptographic algorithms are specified in [Annex A](#). These metrics concern first-order attacks (as opposed to high-order attacks, for which there is no consensual modulus operandi). The important parameter in the measurements is the  $S/N$  of the artefact and its operating environment.