FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEC
FDIS
17825**

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2023-09-01

Voting terminates on:
2023-10-27

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

Reference number
ISO/IEC FDIS 17825:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

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

This second edition cancels and replaces the first edition (ISO/IEC 17825:2016), which has been technically revised.

The main changes are as follows:

- test methods have been updated as per research trends;
- an introduction has been added which states the expectations in terms of security level of this document;
- requirements have been numbered to ensure their traceability.

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 and www.iec.ch/national-committees.

Introduction

Testing requires defined constants, which are derived from an axiomatic analysis of the security problem. The security assurance levels are bound to the testing and remaining risks. The testing approach can be characterized as follows:

a) Testing soundness

   1) A formal description of empirical closed-box testing provides the soundness, in the context of the attack, because the testing adheres to an accepted methodology.

   2) The application of the methodology does not ensure that all possible attacks are covered. Testing allows for weakness detection in a system; hence, it increases the confidence in a system's ability to withstand a set of simulated attacks. The implemented formalism allows to detect weaknesses, and the outcome is a reasonable level attested by tests.

   3) The level of assurance that can be reached with the methodology in this document is a “controlled” level of “reasonable” confidence level, which is the level low to medium. Level high is not reachable due to the closed-box approach. The meaning of “reasonable” is determined by the customer's risk threshold. The tester is defining the level of reasonability, in accordance with a security level target.

   4) Testing is guided by a strategy, which allows for transparency in the methodology and outcomes.

   5) The methodology is device-class specific. The pass/fail criteria should take into account the class of devices under test. For example, the criteria for devices with a deterministic behaviour (i.e. bare metal), and for devices with a complex software stack should be different.

   6) Security testing is an “estimation” when based upon noisy measurements, or when the tester does not have full control of the implementation under test (IUT).

b) Repeatability (as per ISO/IEC 17025:2017, 7.2.2.4)

   Repeatability means similar results from the same (i.e. repeated) methodology, while reproducibility means similar results from similar methodology. Security evaluation is an estimation based on noisy measurements, on IUT whose behaviour is probably not in full control of the tester. In this document, there is a prerequisite that the IUT is closed-box, which can behave in a non-deterministic manner (at least, its internals – owing to some intentional randomization used as a protection). Furthermore, the test can only be carried out based on external observations and findings. As a result, the objective is to document a formal and transparent process of testing, where independent tests can be reproduced with similar expected results (as much as possible, within reasonable bounds). The methodologies are similar (e.g. executed by two testers) in that they yield similar outcome.

c) Cost of testing

   1) The objective is to devote the right amount of effort for the testing of a given assurance level. Cost effectiveness of the testing has a direct implication on assuring a certain level of security. Cost of testing includes, but is not limited to:

      i) Level of expertise and experience: Consequence/implication of using an already formalized process (agnostic in the IUT). The testers require skills and competencies.

      ii) Time: Elapsed time for data acquisition, even though the procedure is automated.

      iii) Equipment: The cost impact of equipment is covered in ISO/IEC 20085-1:2019 (requirements) and ISO/IEC 20085-2:2020 (calibration).

   2) This document aims to keep cost moderate. A threshold is reached in the assurance level up to a certain number of traces captured. The level of assurance does not increase significantly more

beyond the threshold. The prescribed methodology cannot exceed a certain level of assurance by its design.

The following statements apply as an artifact of the methodology used:

d) Closed-box testing limits this methodology to exclusively test for leakage that does not account for specific features of a given algorithm's implementation (e.g. implementation specificities, such as parallel execution of unrelated cryptographic operations, or countermeasures, such as random masking, implementation of field arithmetic in elliptic curve cryptography).

e) Testing only considers leakage during tested cryptographic operations using keys. By design the process does not look for other potential sources of leakage (e.g. emissions during transit of keys over internal bus).

f) Results are dependent on the data sets and quality of equipment used during acquisition. Attackers with larger resources can still exploit attack paths tested by this methodology, even if they had passed the test based on increased resources and effort.

g) More sophisticated attacks can be applied and succeed. More sophisticated attacks refer to attacks other than conventional ones, for example the attacks that are particular to asymmetric ciphers (see 9.2).

h) Each specific application/cryptographic module API instance also requires a delta evaluation on top of the generic tests in this document. Such areas of assessment should include application-specific non-parametric module usage threats, such as traffic analysis, manipulation of logical order or scope of external operations.

In this document, requirements are numbered. By convention, the requirements are labelled as [CC.NN], where CC represents the clause number (e.g. 06 means Clause 6), and NN represents the requirement position within the Clause (e.g. the first requirement of Claude 6 is referred to as [06.01]). The purpose of labelled requirements is to ease the generation of documents showing compliance with this document, and their traceability for testers.

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

1 Scope

This document specifies the non-invasive attack mitigation test metrics for determining conformance to the requirements specified in ISO/IEC 19790:2012 for security levels 3 and 4. The test metrics are associated with the security functions addressed in ISO/IEC 19790:2012. Testing is conducted at the defined boundary of the cryptographic module and the inputs/outputs available at its defined boundary.

This document is intended to be used in conjunction with ISO/IEC 24759:2017 to demonstrate conformance to ISO/IEC 19790:2012.

NOTE ISO/IEC 24759:2017 specifies the test methods used by testing laboratories to assess whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790:2012 and the test metrics specified in this document for each of the associated security functions addressed in ISO/IEC 19790:2012.

The test approach employed in this document is an efficient "push-button" approach, i.e. the tests are technically sound, repeatable and have moderate costs.

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*

ISO/IEC 24759:2017, *Information technology — Security techniques — Test requirements for cryptographic modules*

3 Terms and definitions

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

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

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at https://www.electropedia.org/

3.1
advanced side-channel analysis
ASCA
advanced exploitation of the instantaneous side-channels emitted by a cryptographic device that depends on the data it processes and on the operation it performs to retrieve secret parameters

3.2
correlation power analysis
CPA
analysis where the correlation coefficient is used as the statistical method

3.3
critical security parameter class
CSP class
class into which a *critical security parameter* (3.3) is categorised

EXAMPLE Cryptographic keys, authentication data such as passwords, PINs, biometric authentication data.

3.4
differential electromagnetic analysis
DEMA
analysis of the variations of the electromagnetic field emanated from a cryptographic module, using statistical methods on a large number of measured electromagnetic emanations values for determining whether the assumption of the divided subsets of a secret parameter is correct, for the purpose of extracting information correlated to security function operation

3.5
differential power analysis
DPA
analysis of the variations of the electrical power consumption of a cryptographic module, for the purpose of extracting information correlated to cryptographic operation

3.6
electromagnetic analysis
EMA
analysis of the electromagnetic field emanated from a cryptographic module as the result of its logic circuit switching, for the purpose of extracting information correlated to security function operation and subsequently the values of secret parameters such as cryptographic keys

3.7
implementation under test
IUT
implementation which is tested based on non-invasive methods

3.8
power analysis
PA
analysis of the electric power consumption of a cryptographic module, for the purpose of extracting information correlated to the security function operation and subsequently the values of secret parameters such as cryptographic keys

3.9
side-channel analysis
SCA
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

3.10
side-channel collision attack
powerful category of *side-channel analysis* (3.9) that usually combines leakage from distinct points in time, making them inherently bivariate

3.11
simple electromagnetic analysis
SEMA
direct (primarily visual) analysis of patterns of instruction execution or logic circuit activities, obtained through monitoring the variations in the electromagnetic field emanated from a cryptographic module, for the purpose of revealing the features and implementations of cryptographic algorithms and subsequently the values of secret parameters

3.12
simple power analysis
SPA
direct (primarily visual) analysis of patterns of instruction execution (or execution of individual instructions), in relation to the electrical power consumption of a cryptographic module, for the purpose of extracting information correlated to a cryptographic operation

3.13
timing analysis
TA
analysis of the variations of the response or execution time of an operation in a security function, which can reveal knowledge of or about a security parameter such as a cryptographic key or PIN

4 Symbols and abbreviated terms

ASCA	advanced side-channel analysis
AES	advanced encryption standard
CPA	correlation power analysis
CSP	critical security parameter
DEMA	differential electromagnetic analysis
DES	data encryption standard
DLC	discrete logarithm cryptography
DPA	differential power analysis
DSA	digital signature algorithm
ECC	elliptic curve cryptography
ECDSA	elliptic curve digital signature algorithm
EM	electromagnetic
EMA	electromagnetic analysis
HMAC	keyed-hashing message authentication code
IFC	integer factorization cryptography
IUT	implementation under test
MAC	message authentication code
PA	power analysis
PC	personal computer
PCB	printed circuit board
PKCS	public-key cryptography standards
RBG	random bit generator
RNG	random number generator

RSA	Rivest Shamir Adleman
SCA	side-channel analysis
SEMA	simple electromagnetic analysis
SHA	secure hash algorithm
SNR	signal to noise ratio
SPA	simple power analysis
USB	universal serial bus
TA	timing analysis
·	multiplication symbol

5 Document organization

Clause 6 specifies the non-invasive attack methods that a cryptographic module shall mitigate against for conformance to ISO/IEC 19790:2012.

Clause 7 specifies the non-invasive attack test methods.

Clause 8 specifies the test methods for side-channel analysis of symmetric-key cryptosystems.

Clause 9 specifies the test methods for side-channel analysis of asymmetric-key cryptosystems.

This document shall be used together with ISO/IEC 24759:2017 to demonstrate conformance to ISO/IEC 19790:2012.

6 Non-invasive attack methods

This clause specifies the non-invasive attack methods that shall [06.01] be addressed to ensure conformance with ISO/IEC 19790:2012.

The non-invasive attacks use side-channels (information gained from the physical implementation of a cryptosystem) emitted by the implementation under test (IUT), such as:

- the power consumption of the IUT,
- the electromagnetic emissions of the IUT,
- the computation time of the IUT.

The number of possible side-channels can increase in the future (e.g. photonic emissions,[49] acoustic emanations).

In order to be more formal in the taxonomy of the attacks, a formalism allows the relationships to be highlighted between the different attacks and to have a systematic way to describe a new attack.

An attack is described in the following way:

<KKK>-<YYY>-<XXX>-<ZZZ>-<TTT>

KKK refers to the order of the attack (e.g. “2O” for second order attack).

YYY refers to the statistical treatment used in the attack (e.g. "S" for simple, "C" for correlation, "MI" for mutual information, "ML" for maximum likelihood, "D" for difference of means, "LR" for linear regression, etc.).

NOTE 1 Other statistical treatments can be inserted like "dOC" which corresponds to a correlation treatment exploiting *d*th order moments (obtained for instance, by raising each targeted point in the traces to a power *d*, or by combining *d* points per trace before processing the correlation).

XXX refers to the kind of observed side channel: e.g. "PA" for power analysis, "EMA" for electromagnetic analysis, "TA" for timing analysis, etc.

ZZZ can refer to the profiled ("P") or unprofiled ("UP") characteristic of the attack. This is optional and the default value is "UP".

TTT refers to the direction of the attack (e.g. "V" for vertical, "H" for horizontal,[43] "R" for rectangle).

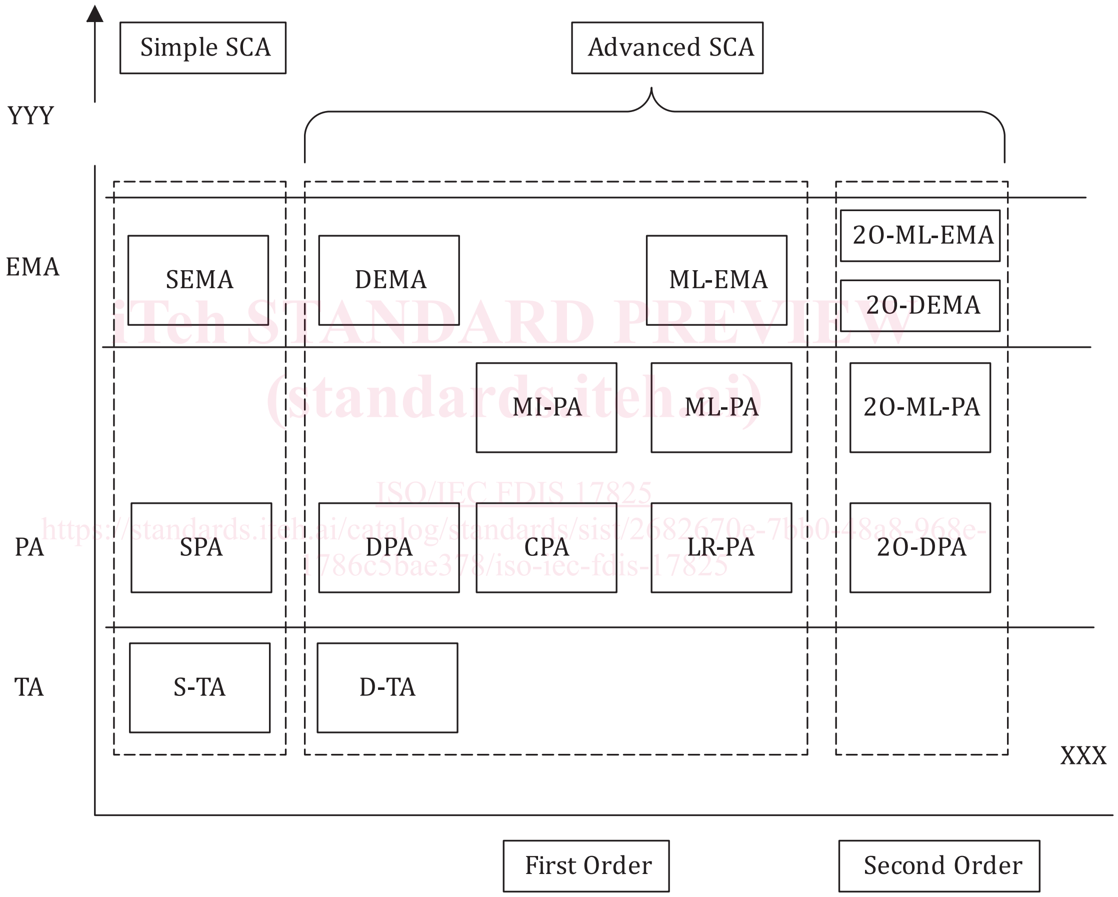

Figure 1 — Taxonomy of non-invasive attacks

NOTE 2 Instead of just splitting advanced side-channel analysis (ASCA) into univariate and multivariate cases, the classification can still be refined by separating attacks based on "variable distinguishers" (which focus on a particular moment of the distribution of the target variable) from those based on "pdf distinguishers" (non-invasive analysis distinguisher which requires as input an estimation of the leakage probability density function knowing the secret key). The first category includes ASCA based on correlation or on the linear regression techniques. The second one includes maximum likelihood and mutual information attacks for instance.

NOTE 3 The simple power analysis (SPA) and simple electromagnetic analysis (SEMA) attack methods include some extensions to basic SPA and SEMA attacks (i.e. template attack). The differential power analysis (DPA) and differential electromagnetic analysis (DEMA) attack methods include some extensions to basic DPA and DEMA attacks [i.e. correlation power analysis (CPA) and higher-order DPA attacks]. It is not mandatory to test them in this document.

The taxonomy of non-invasive attacks is illustrated in Figure 1. The scope of this document focuses on first-order attacks, i.e. the first two columns of Figure 1. Emerging non-invasive attacks and side-channels are described in Annex D but are not applicable currently as required test method in this document.

The variables used in the description of ASCA are:

A	cryptographic processing
C	observation processing
D	number of predictions
d_C	multivariate degree
d_D	multivariate degree
d_o	dimension of observation
F	function, i.e. manipulation
h	observation
i	index
K	secret key
*k*1	sub key 1
*k*2	sub key 2
M	model of leakage
N	number of observations
o_i	observation interval
(*o_i*)*_i*	observation interval number *i*
pred_i	prediction
t_i	*i* iteration of time
*x*1*_i*	*i* iteration of *x*1
*x*2*_i*	*i* iteration of *x*2
X	known data

ASCA is described in the following steps:

1) Measure *N* observation intervals *o_i* related to a cryptographic processing *A* parameterized by a known input *X* and a secret key *K*.

2) (Optional) Choose a model of leakage *M* for the device leakage.

3) (Optional) Choose an observation processing *C* (by default *C* is set to the identity function).

4) Make all hypothesis *h* on the value of *K* or a subpart of it.

5) Select as the most likely key the hypothesis with the largest statistical test.

NOTE 4 The observations o_i can be univariate or multivariate. In the latter case, each coordinate of o_i, viewed as a vector, corresponds to a different time t_i. The dimension of o_i is denoted by d_o in the rest of this note.

NOTE 5 In side-channel collision attacks against block ciphers, the second step is skipped and the third step simply consists in a point selection in the traces o_i. Then, the hypothesis h typically corresponds to a hypothesis between the difference (k1-k2) of two parts of the targeted key K (e.g. two sub-keys in a block cipher implementation). Eventually, the predictions are deduced from the observations (o_i)_i and the difference h. If for instance the attack targets the manipulation of a value F(x1_i+k1) [i.e. C(o_i) corresponds to the part of the observation related to the manipulation of F(x1_i+k1)], then the attack will extract from the o_i the observations during the manipulation of another values F(x2_i+k2). Those observations will be re-arranged such that x2_i – x1_i = h. Then h_i corresponds to the part of the observation related to the manipulation of F(x2_i+k2) = F(x1_i+k1) if h is correct. To validate the hypothesis, a correlation coefficient is usually used for D. Additionally, all the attacks described in Clause 6 can be vertical, horizontal or rectangle (i.e. horizontal and vertical). An attack is said to be vertical if each observation o_i corresponds to a different algorithm processing. If all the o_i correspond to a same algorithm processing, then the attack is said to be horizontal. If some o_i share the same algorithm processing while some other o_i do not, then the attack is said to be rectangle. The classical attacks specified in literature are vertical and this modus operandi will hence be defined as the default one. Examples of attacks performed in the horizontal mode can be found in References [43] and [44].

NOTE 6 An approval authority can modify, add or delete non-invasive attack methods, the association with security functions (see Table C.1) and non-invasive attack mitigation test metrics specified in this document.

7 Non-invasive attack test methods

7.1 General

This clause presents an overview of the non-invasive attack test methods for the corresponding non-invasive attack methods specified in Clause 6.

7.2 Test strategy

The goal of non-invasive attack testing is to assess whether a cryptographic module utilizing non-invasive attack mitigation techniques can provide resistance to attacks at the desired security level. No standardized testing programme can guarantee complete protection against attacks. Rather, effective programmes validate that sufficient care was taken in the design and implementation of non-invasive attack mitigations.

Non-invasive attacks exploit a bias latent in the physical quantities which are non-invasively measured on or around the IUT. Such a bias is induced from and depends on the secret information that the attacks target. For further details, see Reference [16]. The bias can be subtle but is generally persistent. In this document, the biased information that depends on the secret information is referred to as leakage hereinafter. A device can fail one or more tests if experimental evidence suggests that leaking information exceeds permitted leakage thresholds. This implies that leakage demonstrates a potential vulnerability. Conversely, attacks fail and the test passes unless leakage is observed. The test of existence of leakage is called leakage analysis (leak analysis) hereinafter.

The goal is to collect and analyse measurements within certain test limitations such as maximum waveforms collected, elapsed test time, and to determine the extent of the CSP information leakage. The test limitations and leakage thresholds constitute the test criteria. The maximum acquisition time shall [07.01] also be bounded. The values for security Level 3 and Level 4 are detailed in Annex A.

Consider timing the attack testing. If the test reveals that the computation time is biased relative to the CSP, the IUT fails. For DPA, if the test reveals that the power consumption during CSP-related processes is biased relative to the CSP, the IUT fails. The testing approach uses statistical hypothesis testing to determine the likelihood that a bias is present. Thus, this document provides a leakage threshold in terms of statistical significance. The test fails if a bias exceeds the leakage threshold. The pass/fail conditions for the desired security level are given in Annex A.