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)

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

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

3.3
application-specific tool
tool dedicated to the measurements and analyses required by ISO/IEC 20085 (all parts)

Note 1 to entry: Antonym of laboratory-assembled tool.

3.4
batch measurement
measurement that includes signals related to repeated execution of one cryptographic operation with a single or with different inputs

Note 1 to entry: See Figure A.1.

3.5
cartography
procedure involving placing a sensor at various positions and taking measurements at each of them to create a spatial (or visual) representation of some data

Note 1 to entry: See A.8.

3.6
horizontal attack
HA
modus operandi where sensitive information is extracted from a single measurement split into several parts

Note 1 to entry: The single measurement can be an averaged measurement obtained from a batch of measurements where repeated operations are conducted with the same cryptographic inputs.

[SOURCE: ISO/IEC 17825:2016, 3.8, modified — Note to entry has been added.]

3.7
implementation under test
IUT
implementation which is tested based on methods specified in ISO/IEC 17825:2016

[SOURCE: ISO/IEC 17825:2016, 3.9, modified — The words “in this International Standard” have been replaced with “in ISO/IEC 17825:2016”.]

3.8
laboratory assembled tool
tool made by assembly of commercial off-the-shelf (COTS) products

Note 1 to entry: Antonym of *application-specific tool* (3.3).

3.9
measurement tool
test tool component with the ability to measure signals in digital format (scalar or vector), time-synchronized with a trigger signal, and that records permanently or transiently the measurements for subsequent analysis

3.10
multivariate trace
trace made up of several samples

EXAMPLE The measurement of an electromagnetic field over time is a multivariate trace.

Note 1 to entry: Usually, a “trace” is considered multivariate.

3.11
non-invasive attack
attack that can be performed on a cryptographic module without direct physical contact with components within the cryptographic boundary of the module

Note 1 to entry: An attack that does not alter or change the state of the cryptographic module.

[SOURCE: ISO/IEC 19790:2012, 3.78]

3.12
signal-to-noise ratio
S/N
measure that compares the level of a desired signal to the level of background noise

Note 1 to entry: It is defined as the ratio of signal power to the noise power.

[SOURCE: ISO/IEC 27033-6:2016, 3.8, modified — The abbreviated term has been added.]

3.13
univariate trace
trace made up of one sample

EXAMPLE A measurement of duration is a univariate trace.

3.14
vertical attack
VA
modus operandi where sensitive information is extracted from different algorithm executions

Note 1 to entry: If the algorithms executions are the same, then the traces can be averaged in a view to increase their *signal-to-noise ratio* (3.12), and then a *horizontal attack* (3.6) can be carried out.

Note 2 to entry: The definition is equivalent to: "Modus operandi where sensitive information is extracted from measurements of repeated execution of one cryptographic operation with different inputs".

[SOURCE: ISO/IEC 17825:2016, 3.17, modified — Notes to entry have been added.]

4 Symbols and abbreviated terms

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

API Application Programming Interface

COTS Commercial Off-The-Shelf

CSP Critical Security Parameter

SPA Simple Power Analysis

5 Test tools

5.1 General

ISO/IEC 20085 (all parts) relates to ISO/IEC 17825:2016, which specifies the non-invasive attack mitigation test metrics for determining conformance to the requirements specified in ISO/IEC 19790 for Security Levels 3 and 4. The test metrics are associated with the security functions specified in ISO/IEC 19790.

This document also relates to ISO/IEC 20085-2, which details how the test tool shall be calibrated, to adjust to the requirements (threshold values, for Security Levels 3 and 4) of ISO/IEC 17825.

5.2 Types of side-channels

5.2.1 General

ISO/IEC 17825:2016, Clause 6, specifies three types of side-channels concerned with non-invasive attacks, namely:

a) the power consumption of the IUT,

b) the electromagnetic emissions of the IUT, and

c) the computation time of the IUT.

These side-channels are represented in Figure 1, and are addressed in the Introduction, 5.2.2, 5.2.3 and 5.2.4. These side-channels are measured passively insofar as the IUT behaviour is not disturbed by the measurement tool.

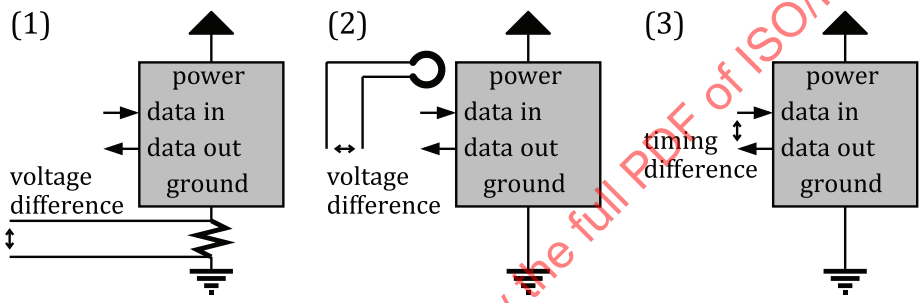

Figure 1 — Three types of side-channels

Other types of side-channels are emerging (see ISO/IEC 17825:2016, B.6).

5.2.2 Power consumption

The power side-channel can be measured by various means. Power measurements are typically measured as a voltage difference.

5.2.3 Electromagnetic emissions

The measurement is indicated by a voltage difference measured by an antenna. Therefore, the measurement can be carried out remotely, and without contact with the cryptographic module.

5.2.4 Computation time

The measurement is indicated by a difference of timing for the selected cryptographic operation, obtained as the subtraction of times corresponding to the cryptographic resources to triggers (*start* and *end*).

5.3 Categorization of test tool

Test tools can be broadly categorized in two types: "Laboratory Assembled", and "Application Specific".

— For Laboratory Assembled tools the non-invasive attack test tool is assembled from two or more commercial off-the-shelf (COTS) products, each of which can have another purpose in the laboratory.

— Application Specific tools, which can also be available as COTS products are dedicated to the measurements and requirements of ISO/IEC 20085 (all parts). They cannot be used for other laboratory testing tasks.

NOTE A test tool is not necessarily a crafted tool. It can be built from parts of equipment used in other contexts.

5.4 Test tool components

5.4.1 General

A test tool is made up of two components: a measurement tool and an analysis tool. Their requirements are detailed in this subclause.

5.4.2 Measurement tool

Measurement tools are required to collect the side-channel emanations from the IUT. There shall be at least two measures: time (horizontal side-channel) and voltage/electromagnetic field (vertical side-channel).

The measurement tools can be two distinct tools i.e. a timer and a digitizer. Both functions can be presented by a single tool (e.g. an oscilloscope), which is able to measure vertical quantities as well as timing as a "function" feature. Such a setup can perform all the tests found in ISO/IEC 20085 (all parts) serially without the need for hardware setup reconfiguration. The single-tool solution is recommended as more convenient for the tester and supports accuracy since the experimental conditions are maintained unchanged during the whole test procedure.

Such measurement tool shall reflect the internal operations carried out within the IUT. For instance, the horizontal side-channel shall relate to the number of required computations, while the vertical side-channel shall show up when a critical security parameter (CSP) is used. In this second case, the CSP can directly influence the vertical side-channel, or indirectly, e.g. because it is mixed with parts of the plaintext/ciphertext (assuming the operation is a symmetrical encryption).

Horizontal side-channel can be measured as the duration between a request and a response. However, unpredictable latency can decrease the S/N of such measurement. A more accurate option consists in the derivation of the operation duration from a vertical side-channel trace. In this case, the actual duration can be measured[5]. The sensor involved is a timer. The test requirements listed in ISO/IEC 17825 demand a resolution less than or equal to the clock frequency of the cryptographic module making up or embedded in the IUT.

Vertical side-channel can be measured either globally or locally. Global vertical side-channel measurement consists in the acquisition of an aggregate quantity, e.g. the total power consumption of the whole IUT. This method is well suited for single-chip modules. Local vertical side-channel measurement consists in using a sensor smaller than the IUT, which is placed at various locations around or inside the IUT, where the S/N is stronger. This procedure is referred to as a cartography (see details in A.8). It is a preferred method for the localization of the leakiest position in the case the IUT is a multi-chip module. The sensor shall be able to probe leaked information without tampering with the IUT.

Examples of such sensors are:

— an antenna (microscopic, mesoscopic or macroscopic) which measures the electromagnetic field emitted by the IUT;

— a current probe placed on the communication or power cables of the IUT can measure leakage outside the boundary of the IUT[6].

An illustration of horizontal versus vertical attacks, and univariate traces versus multivariate traces, is given in Figure 2.

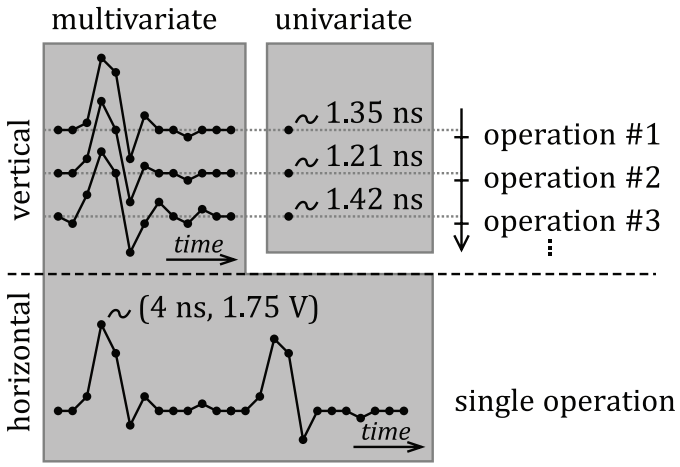

Figure 2 — Illustration of vertical versus horizontal attacks, and multivariate versus univariate side-channel traces

Horizontal side-channel analysis shall be performed with one single measurement and shall be collected as noise-free as possible. Such analyses include asymmetric cryptography where the security parameter is updated upon each cryptographic operation, or symmetrical cryptography which can be analysed using a profiled attack (also known as a "template" attack). Regarding vertical side-channel analysis, the S/N can be enhanced by adding more traces. If the noise is independent from one measurement to the next, the S/N (in power) increases linearly with the number of measurements. Therefore, setup quality can be traded for more measurements in vertical side-channel analysis. In addition, vertical side-channel analyses require traces to be properly aligned, otherwise the contrast of the analysis is reduced. The traditional modus operandi when both horizontal and vertical analyses are prescribed:

— first a horizontal analysis is carried out: if the control flow depends on the key, then it is likely to be exploitable at this stage;

— otherwise, the control flow does not depend on the key material, therefore traces are (by design) aligned, which is a favorable situation for vertical side-channel analyses.

Environmental conditions shall be carefully monitored during the measurements. The external environment conditions shall be controlled as they can influence the side-channel emanation changes during the measurements; temperature and supply voltage shall be monitored as specified in ISO/IEC 19790:2012, 7.7.4.3. The measurement tool shall be stable. For example, some oscilloscopes require some warm up time after power-up to carry out reproducible and accurate measurements. Symmetrically, the IUT shall be powered up sufficiently in advance so that it has reached a stable state, allowing for measurements with as little trend noise as possible.

An example of measurement tool and its attributes can be found in Annex B.

Measurement of power consumption (see 5.2.1), electromagnetic emanations (see 5.2.2) and computation time can be carried out as explained below.

a) Power consumption measurements are carried out across a current probe or a conductor that is inserted between the measurement ground (or voltage supply) and that of the IUT. The conductor can be a resistor (or, respectively, a capacitance, or an impedance), in which case the measurement is a voltage difference, proportional to the current drawn by the resistance (or, respectively, proportional to its integral or derivative). The acquired signal can be amplified. Depending on the targeted algorithm, the trace:

   1) can focus on the first (or the last) clock cycles of the cryptographic operation [case of ASCA on symmetric encryption, where the plaintext (or the ciphertext) is known];

2) encompasses the whole operation, as is the case of HA on asymmetric cryptography.

b) As for power consumption, the electromagnetic signal can be amplified. The location of probe is an important parameter. In a view to optimize the S/N, a cartography can be done. It can scan over the chip die, or the whole printed circuit board (PCB), including decoupling capacitors.

c) Computation time measurement can be carried out in a variety of way. A first option is the timing difference between the time when the operation is launched, and result is returned. A second option is the timing difference between the cryptographic modules start and stop, observed for instance from a multivariate side-channel trace, be it power or electromagnetic side-channel. In this respect, the measurement consists in a post processing of a power or of an electromagnetic emission measurement.

5.4.3 Analysis tool

The analysis tool is made up of three components.

The first component controls the measurement process. This is an automation task which can be implemented in several ways e.g. through a scripting language or through use of a more advanced program. This control can simply request traces sequentially. However, when a large number of measurements is required, batch measurement can be useful (refer to A.7).

The second component is data post-processing where the recorded measurements are conditioned to:

— remove abnormal traces (clearly invalid traces identified as outliers are filtered out);

— alignment[9] using points of interest within the traces (this step is natural for vertical attacks; however, it is also beneficial to horizontal attacks when the trace is obtained from an averaging of identical operations);

— reduce the dimensionality, thanks to principal components analysis (PCA), linear discriminant analysis (LDA) or variance tests [for data compression, statistics (e.g. probability density function) simplification, and computation load alleviation];

— allow for data fusion, especially in the case of multi-sensor or multiple modality (e.g. power and electromagnetic field concomitant measurements, refer to Bibliographic references[3] and[4]).

Such post-processing is typically carried out by a software program. It can require a caching of the measurements. The purpose of the cache is to provide a local temporary storage of part, or all, of the measurements.

The third component analyses the post-processed data in order to identify any valid attacks. The methodology is explained in ISO/IEC 17825. The goal of this tool is to verify that the measurement and the analysis were carried out properly. It consists in a CSP recovery attack, where the obtained CSP is checked for consistency with the known plaintexts/ciphertexts.

5.4.4 Functional items of test tools components

Measurement tool is comprised of the following items.

— Probes: they are sensors, which measure a signal. Examples of signals are voltage, current, electromagnetic field, time, photonic emission, etc. They aim at collecting the raw signals.

— Amplifiers: they magnify the signal. In some instances of test tools, the raw signal is quantified (i.e. digitized), therefore its dynamic shall be greater than that of the quantification step, while remaining within the sampling tool range.

— Physical filters: the measured signals are typically noisy. Physical filters can thus remove parts of the noise, while keeping most of the signal. For instance, if the signal is mainly located in one central frequency, then the physical filters can cut or attenuate other frequencies, which are expected to convey only noise. The goal of inserting physical filters is thus to increase the S/N.

— Digitizer and time base (both them can be combined in a COTS product, such as an oscilloscope): the digitizer turns analog signals into digital signals and work along with a time base (separate or integrated) for setting measurement sample rate.

— Trace storage: the captured traces can be stored in a view to be subsequently analysed. The storage can be files, databases, memory buffers, etc.

Analysis tool is comprised of the following items:

— Trace storage: this is a repository where traces, now considered as inputs to the analysis, are saved. This storage can be separate or shared with that of the measurement tool.

— Filtering processing: the noise in the traces can also be removed after measurements. This is the role of filtering. Examples are digital filtering, e.g. with Finite Impulse Response (FIR) filters, which are low-pass (the noise being often, in practice, located in the large frequencies).

— Chaining analysis: the measurement setup can be complex. It is, therefore, important to understand the so-called "measurement channel", for instance to process relevantly the measurements. Examples are inference of noise, intra-trace correlation of samples, etc.

— Frequency analysis: it happens that the signal is hard to spot in the measurements. A time-frequency analysis can help locate the signal in time and according to its main frequency. Examples are spectrograms and a wealth of different scalograms (depending on the mother wavelet).

— Alignment tool: vertical attacks require that traces are aligned in timing. If they are not, it is possible to realign them based on a post-processing[9], which exploits similarities in the traces to match them in terms of timing. Alternatively, traces can be aligned by the analysis of another signal, which would reflect the internal activity of the system (e.g. instruction counter, information from the operating system, etc.).

— Statistical analysis: the signals can be inputs of a statistic test to detect leakage, or to correlate them with a secret-dependent model. These analyses aim at quantifying the amount of leakage conceals in measured traces. Optionally, the statistical analysis can include as a functionality the ability to extract secrets, as in a real attack.

6 Test techniques and associated approaches

6.1 Operation

There are two kinds of collection types.

a) Single measurement [valid for simple power analysis (SPA) tests, the second set of tests mentioned in ISO/IEC 17825:2016, 8.3.2]

b) Multiple measurements, which allows for “ASCA" [required for all other tests, namely Timing Analysis and Differential Power Analysis (DPA), that is the first and third sets of tests mentioned in ISO/IEC 17825:2016, 8.3.2].

The first case is also referred to as horizontal in Figure 2, whereas the second is referred to as vertical. When conducting SPA tests, if the S/N is poor due to environmental conditions, then the testing laboratory can compensate for this by acquiring several measurements for a single input with the sole aim to improve the S/N. The test shall be reproduced at least once by repeating the same operation separated by 6 h, 12 h or 24 h.

In both cases, the measurement tool and the IUT shall be kept synchronized. The collection process consists of the following steps:

— setting up the measurement tool to get ready to acquire data when triggered;

— requesting an operation (possibly a batch operation) from the IUT;

— capturing the data;

— storing the data; and

— transferring the data to the analysis tool, either for local temporary saving or for post-processing.

The trigger can be either a second input of the measurement tool, or the signal itself (e.g. its level, or a series of various levels with a holdoff time between them). In the latter case, only one channel of the measurement tool is required.

Technical considerations to consider during measurement and analysis are listed in Annex A.

6.2 Interaction between the measurement tool and the IUT

The measurement tool and the IUT interact by exchanging commands to activate the cryptographic module and by measuring side-channel during the operation of the cryptographic module. The interface for commands present in general application programming interfaces (APIs) with heterogeneous data encoding conventions, in particular, data type is typically platform-dependent. Therefore, the interface shall handle portable data format.

Besides, some transfers can be comprised of long (highly multivariate) traces. Therefore, interaction benefits from a solution at the measurement tool end which is capable of efficiently serializing large amounts of data. Examples are given in Annex C.

The measured data can optionally be stored by the measurement tool before being handled by the security metric layer (e.g. ISO/IEC 17825). It can be saved as raw traces, or in a database. This second option allows for fast access with optimized data indexing. Examples of efficient data storage are provided in Annex C.

6.3 Interaction between the analysis tool and the IUT

The analysis tools need to have access to input data or output from the IUT, such as plaintext or ciphertext. This information is needed to conduct most non-invasive attacks (except for so-called blind attacks).

6.4 Interaction between the analysis tool and the measurement tool

Notice that there is not always a need for a synchronization between the measurement tool and the analysis tool. There is an interaction when the analysis is carried out on the fly.

Annex A
(informative)

Selection of test methods and approaches

A.1 Understanding of architecture

The leakage depends on the IUT architecture, i.e. the way the data is processed through the device implementation. This subclause details what features of the architecture need to be considered when analysing a design.

NOTE The term "architecture" in this annex has a different meaning from that in ISO/IEC 15408.

a) architecture of CPU:
   1) word width;
   2) endianness for CPUs with word width greater than 8;
   3) clock frequency;
   4) pipelining method, cache and branch prediction mechanisms for launching timing attacks;
b) architecture of data bus:
   1) word width;
   2) clock frequency;
c) architecture of coprocessor:
   1) clock frequency;
   2) symmetric key:
      i) implementation of key scheduling;
      ii) implementation of S-box;
   3) asymmetric key:
      i) underlying algorithm used in modular arithmetic coprocessor;
      ii) method of exponentiation;
d) architecture of RBG;
e) spatial location of blocks (CPU, data bus, coprocessor, RBG);
f) temporal sequence of cryptographic operation:
   1) symmetric key:
      i) key scheduling;
   2) asymmetric key:
      i) ephemeral key generation.

A.2 Leakage model

The knowledge of the architecture helps derive a relevant leakage model, i.e. a leakage model which matches closely with the actual leakage. The procedure typically unfolds as follows:

a) Identify a target sensitive variable. This is a variable which depends on a small (enumerable in reasonable time, e.g. consisting of 1 to 32 bits) part of a CSP, and which can be computed knowing some input (plaintext, ciphertext, etc.)

b) Given the knowledge of the architecture, opt for a suitable transduction between the sensitive variable and a physical quantity. Canonical models are the arithmetic sum of the sensitive variable bits (also known as the Hamming weight model), or the arithmetic sum of the sensitive variable change (also known as the Hamming distance model).

The first step is guided by key subparts which can be guessed independently. For example, in symmetric cryptography, block ciphers such as the AES manipulate its key byte by byte, with a sensitive variable being a guessable byte. In asymmetric cryptography, the key is manipulated by parts which consist in the width of the window (in the case of windows exponentiation algorithms). When several options are possible, it can be advantageously considered to select the one which allows a better discrimination of the key hypotheses. In the context of symmetric cryptography, this often involves a leakage model where the key is processed through a substitution box. Indeed, cryptographic-grade substitution boxes shall resist to several attacks, such as the differential cryptanalysis. Therefore, their differential uniformity is low, which handicaps rival key hypotheses during a side-channel attack[11].

The second step is guided by the knowledge of the IUT architecture. In software implementations, busses can be pre-charged, with a leakage being directly connected to the sensitive variable value, such as its Hamming weight. In other architectures, there is no such pre-charge. For this reason, the change of values is meaningful. Therefore, the leakage consists merely in the Hamming distance between the sensitive variable and another variable known by the evaluator. For instance, in block ciphers, the variable known by the evaluator can be part of the ciphertext, and the sensitive variable can be the predicted value of one byte of the last round key, which depends on one byte of the last round key. Obviously, the choice of the most adequate leakage model requires an “educated guess". But there is no single leakage model so attacks are likely to work, although with more traces, even if the chosen leakage model is not the most adequate (the one which maximizes the S/N and the successful key recovery probability).

Eventually, it is noticed that the key is leaking at many time instants during an algorithm. Each leakage instant can have its own model. Therefore, there is more than one way to select a leakage model.

A.3 Finding high S/N traces

A.3.1 Conditions of test harness

A.3.1.1 Input

a) Selection of supply voltage;

b) Selection of clock signal;

c) "gain", "noise figure".

A.3.1.2 Output

a) Selection of electromagnetic probe:

   1) diameter;

   2) aperture;

3) type of fields that are being measured (normal, coplanar, etc.);

b) Selection of position:

1) orientation;

2) distance from the chip/line.

A.4 Understanding traces

A.4.1 Time domain

It is recommended for testers to understand what the countermeasure is doing in which time domain.

For symmetric key operations, it is interesting to focus on key loading and/or key scheduling. These processes precede actual cryptographic operation (i.e. encryption/decryption).

For asymmetric key operations, it is worthwhile to investigate all operations. For instance:

— in RSA, the leakage can result from the final recombination (when the CRT is used) and not from the modular exponentiation;

— in ECDSA, the leakage can arise from the multiplicative inverse, therefore not from the core of the computation, namely ECC scalar multiplication itself.

Analysis in the time domain can also help "resynchronization"[8][9].

A.4.2 Frequency domain

By applying Fast Fourier Transform (FFT) or spectrum analyser to the traces, the tester can verify that the actual operating frequency emerges as a sharp peak in the spectrum. The peak can be deformed due to the measurement setup or number of points provided.

By applying frequency domain to different spatial locations, the tester can understand where the most significant leakage is. The location is not identified by the global peak in the frequency domain, but by the peak of interest (e.g. coprocessor frequency).

Analysis in the frequency domain is also used for "denoising" (with spectrograms and/or scalograms)[10].

A.5 Flaw hypothesis

Even if the countermeasure claims to implement protections, it is necessary to evaluate them. For instance, masking can be defeated if spurious glitches appear, which couple data from otherwise independent shares.

As another example, even if the dual rail logic is employed, there can be unparalleled rails which can lead to side-channel leakage owing to the routing unbalance.

In general, reasons for the residual leakage can be varied:

— incorrect countermeasure implementation;

— hypotheses in the countermeasure which is not valid in practice;

— optimization of the countermeasure by compilers, which results in their being less efficient or completely removed[12].

A.6 Selection of test methods and approaches

First, an adequate probe is considered that will allow to trade the S/N with accuracy. For example, a microscopic probe will require a lengthy cartography, although a coarser probe will allow a faster cartography, at the expense of a lower S/N (see A.8).

Notice that the communication activity between the test tools and the IUT can introduce noise to the side-channel signal. For S/N improving, it is suggested to mention the passive effect of communication activity to the quality of the side-channel signal.

Second, the need for alignment is considered: do the waveform nicely superimpose? If not, alignment is needed.

After that, a side-channel leakage identification test is carried out on the data: is there an intra-class variance (signal) w.r.t. the intra-class variance (noise)? Such metric is called Normalized Inter-Class Variance (NICV).

In case there is a non-negligible level of NICV, the attack can be safely applied. Otherwise, more traces are needed.

A.7 Optimizing traces acquisition speed and quality with batch measurements

Batch measurements, that is, the capture of the leakage from multiple operations in one single trace, allow to capture more leakage in fewer traces. This technique requires that the IUT be able to carry out chained operations, either natively (like in chained modes of operation) or artificially (through an API). The measurement tool itself is agnostic in this measurement technique. The analysis tool needs to be aware of the relationship between the various operations, so as to derive the proper values being processed upon each operation.

This is illustrated in Figure A.1.

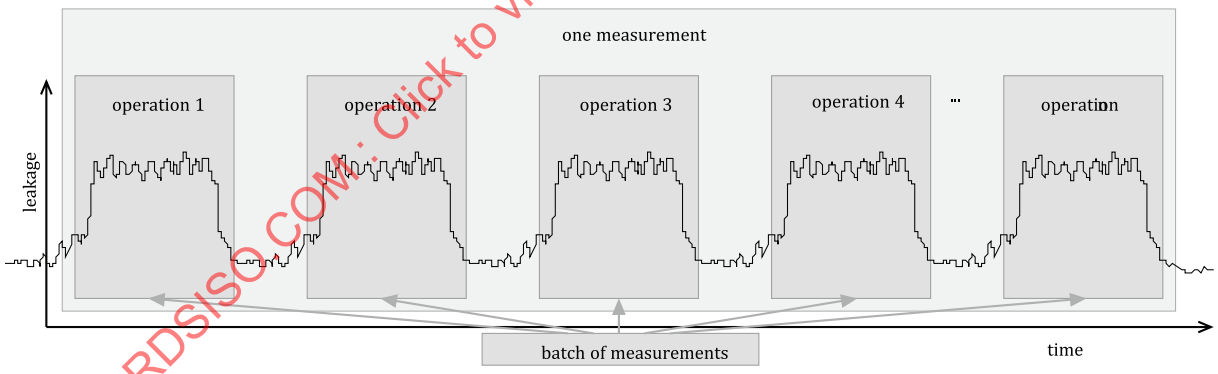

Figure A.1 — Batch of *n* measurements

Batch measurements can be useful to expedite the non-invasive tests when:

— the measurement time is very long, e.g. each measurement requires to reboot the IUT; indeed, measuring as many traces as possible operation traces in one batch measurement allows to make up for the large latency incurred by the boot;

— many measurements are required for the analysis – recall that in ISO/IEC 17825:2016, 11.2 and 11.3, Security Level 3 requires 10 000 measurements, whereas Security Level 4 requires 100 000 measurements, in which case the measurement can be speeded up by a factor *n* (for batches of *n* operations)

— the IUT can only accept a limited number of interactions. Indeed, if the device can only boot a limited amount of times, there is a penalty in taking only one trace per measurement.

In such situations, the IUT can be instructed to perform several operations (e.g. repeated operations with different parameters, or encryption of several blocks of data). Each measure is then split into several individual traces corresponding to single invocations of the cryptographic module. For instance, if a batch of 100 cryptographic operations is performed and measured in each trace, then security testing according to ISO/IEC 17825:2016, Security Level 4 can be achieved with only 1 000 interactions with the IUT.

NOTE From a leakage analysis perspective, it is important how many traces for different inputs are available, not how many interactions with the IUT there are.

A.8 Cartography techniques

Cartography is a measurement process which consists in having the measurement tool displace the probe over the IUT, until it finds a location with sufficient S/N. Classical scanning methods are:

— zigzag (systematic) scanning;

— random scanning (fuzzing);

— gradient-oriented scanning, in the case the S/N can be estimated online.

