INTERNATIONAL STANDARD

ISO/IEC 20085-2

First edition
2020-03

IT Security techniques — Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules —

Part 2: Test calibration methods and apparatus

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

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

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

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **2**
5 Test tools **2**
5.1 Tools and analysis 2
5.2 Determining the test result 2
5.3 Measurement tool 2
5.4 Analysis tool 2
6 Calibration methods **3**
6.1 Aspects 3
6.2 Introduction to calibration procedure 3
6.2.1 General knowledge of calibration procedure 3
6.2.2 Accuracy of test tools 3
6.2.3 Measurement tool 4
6.2.4 Calibration principle 4
6.3 Calibration procedure 4
6.3.1 General 4
6.3.2 Point of measurement 5
6.3.3 Parameter adjustment 5
6.4 Calibration metrics 5
7 Artefact **6**
7.1 General 6
7.2 Side-channel analysis 6
7.3 Open target 6
7.3.1 General 6
7.3.2 General specification 6
7.3.3 Example specification 6
7.4 Closed target 6
Annex A (informative) **Cryptographic algorithms and calibration metrics** **7**
Annex B (informative) **Countermeasures to tune the security strength** **9**
Annex C (informative) **An example artefact implementation — A hardware security module emulated with an FPGA** **11**
Annex D (informative) **An example artefact implementation — A microcontroller** **13**
Annex E (informative) **An example artefact implementation — Signal generator** **15**
Bibliography **16**

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

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

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

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

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

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

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.

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[14]
RSA	Rivest–Shamir–Adleman[15]

5 Test tools

5.1 Tools and analysis

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

5.2 Determining the test result

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

5.3 Measurement tool

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

5.4 Analysis tool

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

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.

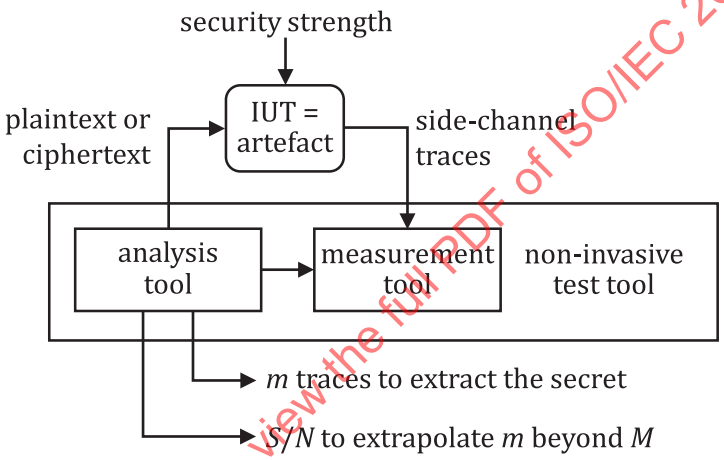


Figure 1 — Block diagram illustrating the relationship between calibration method and non-invasive test tool

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[1]. 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 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 modus operandi). The important parameter in the measurements is the S/N of the artefact and its operating environment.

7 Artefact

7.1 General

A non-invasive test target artefact is a known cryptographic module. Several different non-invasive attack mitigation levels are desired. Due to the calibration principle described in 6.2.4, a non-invasive test target artefact shall be used for the calibration purposes.

7.2 Side-channel analysis

The target artefact shall perform cryptographic operations repeatedly as needed. All the necessary information such as cipher texts shall be provided for the non-invasive side-channel attack method concerned. Likewise, all the necessary physical quantities shall be measured.

7.3 Open target

7.3.1 General

An open target artefact may be used for calibration as described in Clause 6. A cryptographic module with all the design information required to determine the strength level of security against particular attack methods is considered an open target artefact.

7.3.2 General specification

An open target artefact shall have the following properties:

— *S*/*N* properties at electrical contacts: and

— *S*/*N* properties of magnetic field at specified locations.

Guidance can be found in References [5] and/or [6].

7.3.3 Example specification

Annexes B, C, and D show example specifications that meet the general specification described in 7.3.1.

7.4 Closed target

A closed target artefact may be used for calibration as described in Clause 6. Cryptographic modules with known strength levels of security against particular attack methods may be used as calibration artefacts. However, the countermeasures and other implementation information may not be available. In this case, they are called closed target artefacts.

Annex A
(informative)

Cryptographic algorithms and calibration metrics

A.1 Overview

This annex defines the calibration metrics for specific cryptographic algorithms, Security Levels, and attack methods.

A.2 Calibration metrics for selected cryptographic algorithms

A.2.1 AES

A.2.1.1 General

AES is a block cipher which can be typically executed in constant time. Therefore, it is particularly vulnerable to side-channel attacks. Sub-clauses A.2.1.2 and A.2.1.3 reference how the security of an implementation can be measured objectively.

A.2.1.2 DPA

A.2.1.2.1 General

It is possible to measure the *S*/*N* for DPA attacks. From this value, one can derive whether the device is secure or not. According to Equation (1) in B.2., the number of measurements required to break AES is obtained from an algorithmic constant and the given *S*/*N*.

A.2.1.2.2 Security Level 3

Security Level 3 should be tested by the application of Formula (B.3) with M = 10 000.

A.2.1.2.3 Security Level 4

Security Level 4 should be tested by the application of Formula (B.3) with M = 100 000.

A.2.1.3 SPA

A.2.1.3.1 General

For software implementations of AES (which generally execute with less performance the hardware implementations) SPA is a viable attack. The *S*/*N* is evaluated internally of one trace, subsequent to the many calls to the substitution box (SubBytes).

A.2.1.3.2 Security Level 3

Refer to criterion of A.2.1.2.2.

A.2.1.3.3 Security Level 4

Refer to criterion of A.2.1.2.3.

A.2.2 RSA

A.2.2.1 General

RSA, and in general asymmetric cryptographic algorithms, functions with very large numbers. Therefore, it is very time and performance consuming.

A.2.2.2 DPA

A.2.2.2.1 General

DPA can be performed on RSA if the input is not blinded.

A.2.2.2.2 Security Level 3

Refer to criterion of A.2.1.2.2.

A.2.2.2.3 Security Level 4

Refer to criterion of A.2.1.2.3.

A.2.2.3 SPA

A.2.2.3.1 General

RSA is especially prone to SPA attacks since the key is exposed sequentially. Note that the interpretation of the *S*/*N* is detailed in Reference [7].

A.2.2.3.2 Security Level 3

Refer to criterion of A.2.1.2.2.

A.2.2.3.3 Security Level 4

Refer to criterion of A.2.1.2.3.

Annex B
(informative)

Countermeasures to tune the security strength

B.1 Overview

Side-channel attack countermeasures implemented in a cryptographic module are designed to mitigate particular attacks that attempt to gain the information of critical security parameters through side-channel analysis. There are trade-offs between the implementation cost and the effectiveness of mitigation. Trade-offs may be determined by the operating environment of the cryptographic module.

Countermeasures are considered a means to determine the "noise" level and impact on the pass-or-fail test result. The information about the countermeasures can be made available from the vendor of the artefact as specified in ISO/IEC 17825:2016, 8.3.3.

It is known that the number of measurements to extract a critical security parameter such as a key is well approximated by the inverse of the S/N [2]. Therefore, the impact of a countermeasure on the number of measurements can be obtained with the following rule of thumb:

— a countermeasure which shuffles n values or randomly shifts the timing of an operation by n time constants reduces the S/N by a factor equal to n. Therefore, an attacker needs n times more measurements to succeed an attack with the same probability;

— a countermeasure which introduces masking, if correctly implemented, has the effect to change the S/N by the d-th power of the S/N, where d is the order of the masking scheme (that is the number of "shares" the sensitive variables are split into).

B.2 Link between S/N and number of traces to extract the key

Let us call P_S the probability of success in extracting the key. It is explained in Reference [2] that the probability to extract the correct key P_S is converging exponentially to one, according to Formula (B.1):

$$1-Ps=e^{-mE} \tag{B.1}$$

where

m is the number of traces needed to extract the key;

E is a so-called first-order exponent and greater than 0, and given by Formula (B.2):

$$E=\frac{1}{2}\cdot R\cdot \min_{k\neq k^*} K(k^*,k) \tag{B.2}$$

where

R is the signal-to-noise ratio, S/N;

k^* is a secret cryptographic key;

k is a key hypothesis;

$K(k^*,k)$ is a confusion coefficient[3] which depends only on the attacked algorithm.

So, to extract the key with probability P_S = 99 %, the number of measurements m is inverse proportional to the S/N [see Formula (B.3)]:

$$m=\left(\frac{1}{2}\left(R.\min_{k^*\neq k} K\left(k^*,k\right)\right)\right)^{-1}\log\left(\frac{1}{1-0,99}\right) \tag{B.3}$$

EXAMPLE Numerical application on an FPGA.

It is reported in Reference [4] that on an FPGA platform, an AES has leakage such that S/N = 0,007. Therefore, the number of traces to recover the key with P_S = 99 % is about m = 2 600.

— With a shuffling over 16 positions, the S/N is divided by 16. Therefore, m grows to 15 800.

— With first-order masking, the S/N is squared. Therefore, the number of traces grows to m = 376 000.

Annex C
(informative)

An example artefact implementation — A hardware security module emulated with an FPGA

C.1 Overview

This annex provides an example artefact implementation which consists of a printed circuit board equipped with a Field Programmable Gate Array (FPGA), other electronic components, and a circuit representation (bitstream) for the FPGA. The FPGA can contain one or more cryptographic algorithms with known mitigation techniques and acts as the central component of a cryptographic module and, thus, can be considered as a known artefact.

This annex references an open-source project of a suitable artefact which includes various design information and example targets including FPGA implementations.

C.2 Example of differential side-channel attack on FPGAs

An example is an implementation of AES-128 used in the DPA contest v2[8]. This implementation has been studied in detail by more than 40 research teams worldwide. A summary of the performance of submitted attacks is available in Reference [8]. A commented analysis of the possible attacks is given in Reference [9].

Depending on the sophistication level of the attacks, the research shows that the key is recovered with global success rate greater than 80 % in between 700 and 15 000 traces. However, all the attacks do not exploit the same quantity of leakage in their traces. Template attacks improve the success rate significantly. Non-profiled attacks, such as the CPA, can almost unanimously recover the key in M = 10 000 traces.

Therefore, such implementation of AES is suitable for a "borderline" case, meaning that the non-invasive attack test tool recovers the key for Security Level 3.

The Security Level 4 requires 10 times more traces. For this purpose, an implementation of AES-128 with a random start delay which is comprised within uniformly distributed {0, 1, ..., 9} clock cycles are suitable, since it incurs a diminution of S/N by a factor 10.

Eventually, an attack on the first-order masked AES in FPGA requires much more than 1 million traces (the S/N is of the order of 0,001, and for a second-order attack, it is squared and takes the value 1e-6). The FPGA design itself requires a uniform hardware to be run on, which motivates the inclusion of an open platform which can be used as a calibration artefact.

C.3 Design of FPGA target

The FPGA target introduced here is designed to provide a variety of flexible features to allow calibration of tools for testing at different Security Levels. In particular, it provides:

1) a recent FPGA that is expected to be available for the lifecycle of this document;

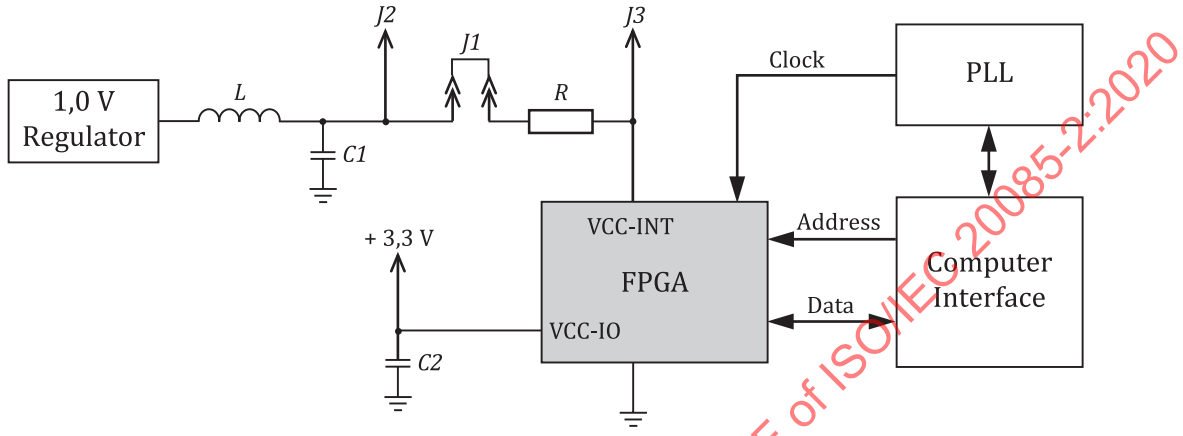
2) a high-speed USB interface for downloading bitstreams and transferring data;

3) an adjustable clocking options independent of FPGA bitstream;

4) a built-in current shunt and amplifier to provide a method of monitoring power consumption with high consistency; and

5) calibration points to help with positioning of EM probes.

This annex describes general design considerations which are useful for implementation of similar artefacts. Figure C.1 depicts the block diagram of a possible artefact with FPGA. An implementation of such an artefact is part of the ChipWhisperer®[1)] project[10] with the CW305 board as the FPGA. Additional details on the construction and use are available as part of that project.



Key

R	shunt resister
L	filter
J1	jumper
J2	measurement point (high side)
J3	measurement point (low side)
C1, C2	decoupling capacitors

Figure C.1 — FPGA Implementation Architecture

Important features of an artefact include a variety of measurement interfaces to assist with calibration of various types of measurement equipment. This can include for example both single-ended and differential measurement points across the shunt resistor in the power supply, along with a capability to insert a jumper wire to use with a current transformer type probe. When using a shunt resistor or similar, decoupling capacitors are not present on the low side of the shunt resistor. The removal of the shunt resistor increases the magnitude of the signal measured across the shunt resistor. A shunt resistor and measurement points are only provided on the power supply for the FPGA's digital logic that is shown as VCC-INT in Figure C.1, and not for the I/O drivers shown as VCC-IO.

The computer interface provides a simple address/data bus to exchange data with the cryptographic core. In addition, an external PLL allows modifications of the cryptographic core clock frequency. This external PLL allows changing of clock frequency without requiring modifications to the FPGA design. This feature is useful for calibration by calibrating the test tool at different clock frequencies according to the artefact.

1) ChipWhisperer® is a trademark of NewAE Technology Inc. and an example of a suitable product available commercially. This information is given in both Annex C and Annex D for the convenience of users of this document and does not constitute an endorsement by ISO or IEC of this product.

Annex D
(informative)

An example artefact implementation — A microcontroller

D.1 Overview

A hardware specification of an example artefact implementation can be defined by an off-the-shelf microcontroller. Such microcontrollers[2)] are available by a variety of manufactures and calibration across a wide variety of devices is useful to ensure a variety of hardware implementations are considered. These devices, available in the open market, have hardware accelerated cryptographic functions, and represent a variety of microcontroller core device types and manufacturers.

Another class of example artefacts are software cryptography implementations that can be programmed on these devices. Such implementations have been posted as part of the DPA Contest v4[11], which includes both example implementations and a wide variety of attacks.

This annex includes an example target for performing the measurements in order to reduce dependence of test results on changes to the artefact design. This annex also includes a description of a suitable artefact. This artefact references an open-source project which includes various design information and example targets including firmware to enable and use various cryptographic accelerators that are part of the provided exemplars. These open targets do include some level of side-channel resistance[3)]. Later parts released to the market allowing usage as an open target artefact are expected to provide improved resistance and may become more suitable as an artefact.

An example functional design description is presented in this annex. The presented target is part of the ChipWhisperer® project, and additional details on the construction and use are available as part of this project. These details can be found in Reference [10].

D.2 Design of microcontroller artefact

The microcontroller artefact example in this annex includes two parts. The first part is the baseboard, which provides a regulated and filtered power supply for microcontroller's core voltage, computer interface, a clock generator, and measurement points. The second part is the IUT target daughter board which has the actual microcontroller and fits onto the baseboard. This configuration allows changing microcontroller targets without requiring considerable effort in changing the microcontroller board itself, and, thus, also enables simple comparisons of different IUT targets while maintaining similar specifications of the support circuitry such as power supply noise and clock frequency.

Example implementations of these boards are found in the ChipWhisperer® project[4)]. The general block diagram of this artefact is shown in Figure D.1.

2) Exemplars of such devices include the STM32F415, the ATSAM4LC2AA, the CEC1702, the MPC5748G, and the MK82FN256VLL15. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC of these products.

3) For example, the ATSAM4LC2AA and MK82FN256VLL15 both references side-channel resistance in the manufacturer-provided datasheet. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC of these products.

4) As the CW308 base board and CW308T target series. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC of these products.