INTERNATIONAL STANDARD

ISO/IEC 17825

First edition
2016-01-15

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 17825:2016(E)

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

Contents

Page

Foreword v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Symbols and abbreviated terms 4

5 Document organization 4

6 Non-invasive attack methods 4

7 Associated Security Functions 7

8 Non-invasive Attack Test Methods 9
8.1 Introduction 9
8.2 Test Strategy 9
8.3 Side-Channel Analysis Workflow 9
8.3.1 Core Test Flow 9
8.3.2 Side-Channel Resistance Test Framework 10
8.3.3 Required Vendor Information 11
8.3.4 TA Leakage Analysis 12
8.3.5 SPA/SEMA Leakage Analysis 13
8.3.6 DPA/DEMA Leakage Analysis 14

9 Side-Channel Analysis of Symmetric-Key Cryptosystems 15
9.1 Introduction 15
9.2 Timing Attacks 15
9.3 SPA/SEMA 15
9.3.1 Attacks on Key Derivation Process 15
9.3.2 Collision Attacks 16
9.4 DPA/DEMA 16
9.4.1 Introduction 16
9.4.2 Test Vectors 18
9.4.3 Detailed Procedure 19

10 ASCA on Asymmetric Cryptography 25
10.1 Introduction 25
10.2 Detailed Side-Channel Resistance Test Framework 27
10.3 Timing Attacks 28
10.3.1 Introduction 28
10.3.2 Standard Timing Analysis 28
10.3.3 Micro-Architectural Timing Analysis 29
10.4 SPA/SEMA 29
10.4.1 Introduction 29
10.4.2 Standard SPA/SEMA 29
10.4.3 Markov SPA/SEMA 30
10.5 DPA/DEMA 30
10.5.1 Introduction 30
10.5.2 Standard DPA/DEMA 30
10.5.3 Address-Bit DPA/DEMA 32

11 Non-invasive attack mitigation pass/fail test metrics 33
11.1 Introduction 33
11.2 Security Level 3 34
11.2.1 Time Limit 34
11.2.2 SPA and SEMA 34
11.2.3 DPA and DEMA 34
11.2.4 Timing Analysis 34

11.2.5 Pre-processing conditions in differential analysis 34
11.2.6 Pass / Fail condition 34
11.3 Security Level 4 35
11.3.1 Time Limit 35
11.3.2 SPA and SEMA 35
11.3.3 DPA and DEMA 35
11.3.4 Timing Analysis 35
11.3.5 Pre-processing conditions in differential analysis 35
11.3.6 Pass / Fail condition 36

Annex A (normative) **Requirements for measurement apparatus** **37**

Annex B (informative) **Emerging attacks** **38**

Annex C (informative) **Quality criteria for measurement setups** **40**

Annex D (informative) **Chosen-input method to accelerate leakage analysis** **42**

Bibliography **43**

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

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

1 Scope

This International Standard 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. Testing will be conducted at the defined boundary of the cryptographic module and I/O available at its defined boundary.

The test methods used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790 and the test metrics specified in this International Standard for each of the associated security functions specified in ISO/IEC 19790 are specified in ISO/IEC 24759. The test approach employed in this International Standard is an efficient “push-button” approach: the tests are technically sound, repeatable and have moderate costs.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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, *Information technology — Security techniques — Security requirements for cryptographic modules*

ISO/IEC 24759, *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.

3.1
advanced SCA
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

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

3.3
critical security parameter
CSP
security related information whose disclosure or modification can compromise the security of a cryptographic module

EXAMPLE Secret and private cryptographic keys, authentication data such as passwords, PINs, certificates or other trust anchors.

Note 1 to entry: A CSP can be plaintext or encrypted.

[SOURCE: ISO/IEC 19790:2012, definition 3.18]

3.4
CSP class
class into which a CSP is categorised

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

3.5
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

3.6
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

3.7
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

3.8
horizontal attack
HA
modus operandi where sensitive information is extracted from a single measurement split into several parts

3.9
implementation under test
IUT
implementation which is tested based on methods specified in this International Standard

3.10
mutual information analysis
MIA
analysis of the mutual dependence of two random variables

3.11
power analysis
PA
analysis of the electric power consumption of a cryptographic module, for the purpose of extracting information correlated to security function operation and subsequently the values of secret parameters such as cryptographic keys

3.12
rectangle attack
RA
modus operandi where the observations acquisition phase mix horizontal and vertical attacks

3.13
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

3.14
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

3.15
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

3.16
timing analysis
TA
analysis of the variations of the response or execution time of an operation in a security function, which may reveal knowledge of or about a security parameter such as a cryptographic key or PIN

3.17
vertical attack
VA
modus operandi where sensitive information is extracted from different algorithm executions

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.

DLC	Discrete Logarithm Cryptography
ECC	Elliptic Curve Cryptography
EM	Electro-Magnetic
HMAC	keyed-Hashing Message Authentication Code
IFC	Integer Factorization Cryptography
MAC	Message Authentication Code
PC	Personal Computer
PCB	Printed Circuit Board
RBG	Random Bit Generator
RNG	Random Number Generator
USB	Universal Serial Bus
*	multiplication symbol
^	exponentiation symbol

5 Document organization

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

Clause 7 of this International Standard specifies for each non-invasive attack method the associated security functions specified in ISO/IEC 19790.

Clause 8 of this International Standard specifies the non-invasive attack test methods.

Clause 9 of this International Standard specifies the test methods for side-channel analysis of symmetric-key cryptosystems.

Clause 10 of this International Standard specifies the test methods for side-channel analysis of asymmetric-key cryptosystems.

Clause 11 of this International Standard specifies the non-invasive attack mitigation pass/fail test metrics for each non-invasive attack method to demonstrate conformance to ISO/IEC 19790.

This International Standard shall be used together with ISO/IEC 24759 to demonstrate conformance to ISO/IEC 19790.

6 Non-invasive attack methods

This clause specifies the non-invasive attack methods that need to be addressed for conformance to ISO/IEC 19790.

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

— Its power consumption,

— Its electromagnetic emissions,

— Its computation time.

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

In order to be more formal in the attacks' taxonomy, a formalism will allow 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:

<YYY>-<XXX>-<ZZZ>

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, etc.).

NOTE 1 Other statistical treatments can be inserted like « dOC » which corresponds to a correlation treatment exploiting dth 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 may refer to the profiled (« P ») or unprofiled (« UP ») characteristic of the attack. This is optional and the default value is « UP ».

Additionally, an adjective may prefix the attack name to refer to the attack modus operandi. It can be: "Vertical" (classical and default mode), "Horizontal" (see [43] for more details about this) or "Rectangle".

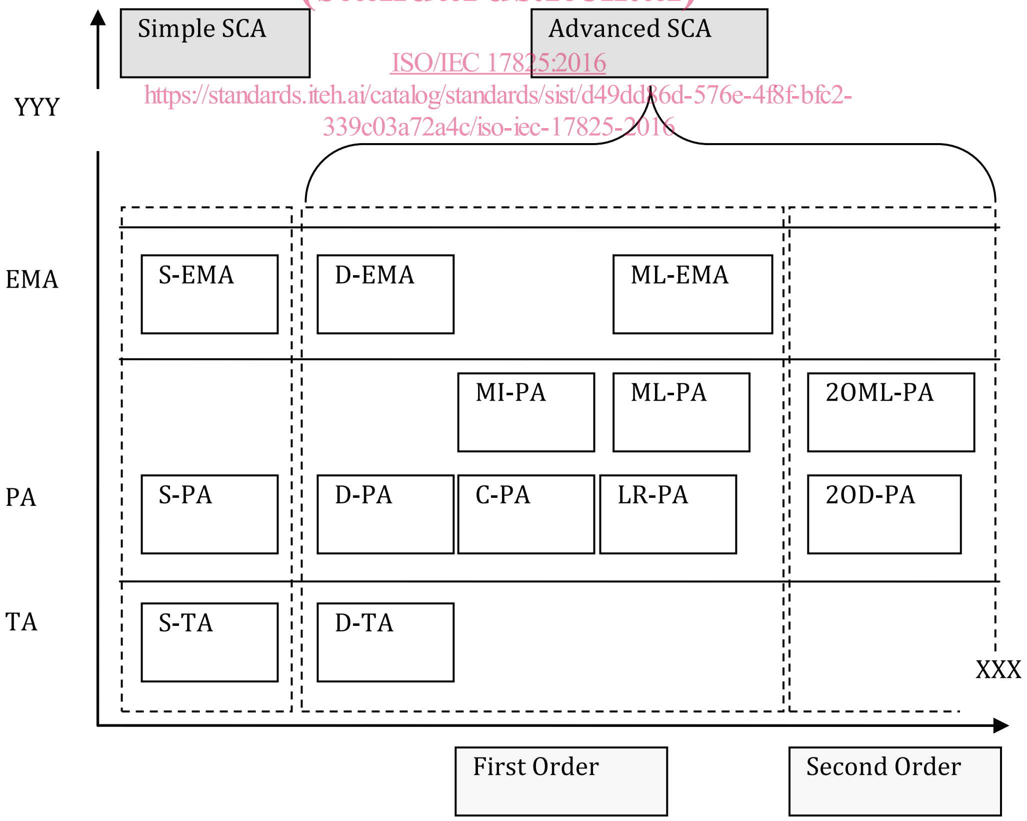

Figure 1 — Taxonomy of non-invasive attacks

NOTE 2 Collision attacks can be viewed as a classical CPA with the single difference that the hypotheses are not deduced from a hypothesis on the way that information leaks from the device but on real measurements that are simply re-arranged in order to (in) validate a hypothesis on a key difference.

NOTE 3 Instead of just splitting ASCA into univariate and multivariate cases, the classification could 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” (which try to distinguish a pdf from another). In the first category we have ASCA based on correlation or on the linear regression techniques. In the second one, we have Maximum Likelihood and MI attacks for instance.

NOTE 4 (informative but not applicable) The SPA and SEMA attack methods include some extensions to basic SPA and SEMA attacks, such as the so called template attack. The DPA and DEMA attack methods include some extensions to basic DPA and DEMA attacks, such as so called Correlation Power Analysis (CPA) and higher-order DPA attacks. It is not mandatory to test them in this International Standard.

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
k1	sub key 1
k2	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
x1_i	i iteration of x1
x2_i	i iteration of x2
X	input text

ASCA is described in the following steps:

a) Measure *N* observations (*o_i*) related to a cryptographic processing *A* parameterized by a known input *X* and a secret *K*.

b) [Optional] Choose a model *M* for the device leakage.

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

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

e) From *A*, *h*, the (*o_i*)*_i* and possibly *M* deduce *N* predictions *pred_i* (one for each value of *X* for which an observation has been measured).

f) Select a statistical test *D* and compute *D* (*pred_i*,*C*(*o_i*)).

g) If *D* (*pred_i*,*C*(*o_i*)) is greater than some threshold, then validate *h*. Otherwise, invalidate *h* and go back to step 4 for a new value *h*.

NOTE 5 In order to stay generic, a threshold value is added in step 7. This threshold should be carefully chosen for an attack to have any chance to succeed. The classical way to choose such a threshold is to take the maximum value, over all key hypotheses, of *D* (*pred_i*, *C*(*o_i*)).

NOTE 6 The observations *o_i* may 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 7 The observation processing *C*(.) can always be defined as a polynomial function over the set of real-valued vectors of size *d_o* (denoted R^{*d_o*}) in the following. The multivariate degree of this polynomial is denoted by *d_C*. Then, the function D(*pred*_i, .): *X* → *D* (*pred*_i, *X*) can also be viewed as a polynomial in *X*. Its multivariate degree is denoted by *d_D*. The value *d_C*d_D* is defined as the order d of the attack. For Mutual Information based attacks, only the degree *d_C* is used to define the attack order: we have *d*=*d_C*.

NOTE 8 In 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*) and 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 this section can be vertical or 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 of the 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 [43] and [44].

NOTE 9 In this International Standard, it is only mandatory to mount vertical attacks.

NOTE 10 An approval authority may modify, add or delete non-invasive attack methods, the association with security functions (see Table 1) and non-invasive attack mitigation test metrics specified in this International Standard.

7 Associated Security Functions

The non-invasive attack methods specified in Clause 6 are associated with the specific security functions that use the CSPs that the attacks target. The security functions are listed in ISO/IEC 19790:2012, Annexes C, D and E.

The associations are shown in Table 1. Other non-invasive attacks and other associations between the attack methods and security functions may exist but defence against them is not currently addressed in this International Standard.

Table 1 — Associations between non-invasive attack methods and security functions covered by this International Standard

Security functions		Non-invasive attack methods		
		SPA/SEMA	DPA/DEMA	TA
Symmetric-Key	AES	A	A	A
	Triple-DES	A	A	A
	Stream Ciphers	A	A	A
Asymmetric-Key	Plain RSA (Key wrapping)	A	A	A
	RSA PKCS#1 v1.5	A	A	A
	RSA PKCS#1 v2.1	NA	NA	A
	DSA	A	A	A
	ECDSA	A	A	A
Hashing mechanisms	SHA	A	NA	NA
RNG and RBG	Deterministic	A	NA	NA
	Non-deterministic	A	NA	NA
Data Authentication Mechanisms	HMAC	A	A	NA
Key Generation		A	NA	NA
Key Derivation from Other Keys		A	A	NA
Key Derivation from Passwords		A	NA	NA
Key Establishment	DLC	A	NA	NA
	IFC	A	NA	NA
Key Entry and Output		NA	NA	NA
Operator Authentication Mechanisms	PIN/Password	A	A	A
	Key	NA	NA	A
	Biometrics	A	NA	A

Legend: A : Applicable, NA : Not-Applicable

NOTE 1 Applicable means that the security functions are susceptible to these types of attacks.

NOTE 2 Not Applicable means that the security functions are not susceptible to these types of attacks.

NOTE 3 An HMAC implementation can be compromised by applying DPA/DEMA, however Block-cipher based MAC will be covered through AES and/or Triple DES.

NOTE 4 All security functions using S Boxes such as AES, Triple-DES etc. can be compromised by applying TA, more precisely cache-timing attacks for software implementations [50].

NOTE 5 RSA PKCS#1 v1.5 can be compromised by applying DPA/DEMA since the used padding is deterministic.

NOTE 6 Timing attacks on RSA PKCS#1 v2.1 are not practicable since the used padding is probabilistic. RSA PKCS#1 v2.1 cannot be compromised by applying DPA/DEMA since the used padding is probabilistic (different random numbers are used for each new signature of the message).

NOTE 7 There are two operations in DSA (resp. ECDSA) that involve the private key or an ephemeral (secret) key:

- The modular exponentiation (scalar multiplication) of a secret value with a known parameter. This operation is vulnerable to simple side-channel analysis and to horizontal differential ones.
- The modular multiplication of a known value and the private key. If the multiplication is implemented in such a way that the multiplier is the private key and the multiplication is carried out with a variant of the binary algorithm, then this implementation is, in principle, vulnerable to side-channel analysis.

NOTE 8 SHA can be used for password hashing e.g. in Password-Based Key Derivation Function, so in this case, a non-protected SHA against SPA/SEMA or DPA/DEMA can lead to the password.

8 Non-invasive Attack Test Methods

8.1 Introduction

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

8.2 Test Strategy

The goal of non-invasive attack testing is to assess whether a cryptographic module utilising non-invasive attack mitigation techniques can provide resistance to attacks at the desired security level. No standardized testing program can guarantee complete protection against attacks. Rather, effective programs 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 non-invasively measured on or around the IUT. Such a bias is induced from and depends on the secret information the attacks target. For background see Reference [16]. The bias may be subtle but is generally persistent. In this International Standard, *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 will fail and the test passes unless leakage is observed. The *test of existence of leakage* will be 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 determine the extent of CSP information leakage. Thus the test limitations and leakage thresholds constitute the test criteria.

Consider timing 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 International Standard provides a leakage threshold in terms of statistical significance. The test will fail if a bias exceeds the leakage threshold.

8.3 Side-Channel Analysis Workflow

8.3.1 Core Test Flow

The tester collects measurement data from the IUT and applies a suite of statistical tests on the collected data. Core test refers to testing for a single security function with a single CSP class, where CSP classes include cryptographic keys, biometric data or PINs. If some security functions deal with more than one CSP class, leakage analysis for every applicable CSP class will be performed for each security function. The test method requires repeating core tests with different CSP classes until the first fail of test occurs or all the CSP classes pass. If a core test is unable to continue if the IUT limits the number of repeated operations, the result is a pass and the core test is continued with the next CSP class. The core test is shown in Figure 2. Side Channel Resistance Test Framework is depicted in Figure 3. Leakage analysis for TA is shown in Figure 4, SPA/SEMA in Figure 5 and DPA/DEMA in Figure 6.