INTERNATIONAL STANDARD

ISO/IEC 20897-2

First edition
2022-05

Information security, cybersecurity and privacy protection — Physically unclonable functions —

Part 2: Test and evaluation methods

Sécurité de l'information, cybersécurité et protection de la vie privée — Fonctions non clonables physiquement —

Partie 2: Méthodes d'essai et d'évaluation

Reference number
ISO/IEC 20897-2:2022(E)

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

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. 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 ISO documents 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 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 20897 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

This document specifies the test methods for physically unclonable functions (PUFs) for generating non-stored cryptographic parameters.

Cryptographic modules generate the certain class of critical security parameters such as a secret key using a random bit generator within the modules. Such modules may store generated security parameters in embedded non-volatile memory elements. For a higher security, a combination of tamper response and zeroisation techniques may be used for protecting stored security parameters from active unauthorized attempts of accessing such parameters. As the reverse-engineering technology advances, however, the risk of theft of such stored security parameters has become higher than ever.

The rapidly pervading technology called a PUFs is promising to mitigate the above-mentioned risks by enabling security parameter management without storing such parameters. PUFs are hardware-based functions providing mathematical unclonability, steadiness and randomness of their outputs and physical unclonability of the functions themselves, taking advantage of intrinsic subtle variations in the device's physical properties, which are also considered objects' fingerprints. PUFs may be used for security parameter (e.g. key, initialization vector, nonce and seeds) generation, entity authentication or device identification in cryptographic modules. More detailed information about the characteristics and security requirements of the PUF are given in ISO/IEC 20897-1 and this document only describes test and evaluation methods.

Now, security requirements of PUFs should be considered at system level, meaning that they should consider many possible attack paths, as detailed further in this document. The purpose of this document is to specify how to test those security requirements for assuring an adequate level of quality of the provided PUFs in cryptographic modules. This document is supposed to be used for the following purposes:

a) In the procurement process of a PUF-equipped product, the procurement body specifies the security requirements of the PUF in accordance with ISO/IEC 20897-1. The product vendor evaluates the PUF in accordance with this document whether the PUF satisfies all the specified security requirements, and reports the evaluation results to the procurement body.

b) The vendors evaluate the security of their PUF in accordance with this document, publicize the evaluation results and clarify the security of their PUF.

It should be noted that all of the security requirements defined in ISO/IEC 20897-1 are not necessarily quantitatively evaluable.

Information security, cybersecurity and privacy protection — Physically unclonable functions —

Part 2: Test and evaluation methods

1 Scope

This document specifies the test and evaluation methods for physically unclonable functions (PUFs). The test and evaluation methods consist of inspection of the design rationale of the PUF and comparison between statistical analyses of the responses from a batch of PUFs or a unique PUF versus specified thresholds.

This document is related to ISO/IEC 19790 which specifies security requirements for cryptographic modules. In those modules, critical security parameters (key) and public security parameters (product serial number, identification code, etc.) are the assets to protect. PUF is one solution to avoid storing security parameters, thereby increasing the overall security of a cryptographic module.

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, *Information technology — Security techniques — Security requirements for cryptographic modules*

ISO/IEC 20897-1, *Information security, cybersecurity and privacy protection — Physically unclonable functions — Part 1: Security requirements*

3 Terms, definitions and abbreviated terms

For the purposes of this document, terms, definitions and abbreviated terms given in ISO/IEC 20897-1, ISO/IEC 19790 and following apply.

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

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1 Abbreviated terms

BER Bit error rate.

iid Independent and identically distributed.

IID

NRBG Non-deterministic random bit generator

4 Symbols

For the purposes of this document, the following symbols apply.

$\forall$ A math symbol representing “for all” or “for any.”

$\in$ A math symbol representing set membership.

$\boldsymbol{D}^{\text{inter}}$ A vector representing Inter-HD between PUF responses.

$\boldsymbol{D}^{\text{intra}}$ A vector representing Intra-HD between PUF responses.

i, j The index for the PUF instances. $1 \leq i, j \leq N_{\text{PUF}}$.

k The index for the challenge. $1 \leq k \leq N_{\text{chal}}$.

N The sequence size (bit length) of PUF responses.

N_{c} The largest number of identical responses (correct responses).

N_{chal} The number of different challenges given to a PUF.

N_{meas} The number of measurements of responses repeatedly collected for a single challenge.

N_{PUF} The number of PUF instances.

N_{res} The length of PUF response obtained from a single challenge.

σ A standard deviation of a random value.

Σ A sum of all values in the specified range.

t The index for the response measurements. $1 \leq t \leq \text{N}_{\text{meas}}$.

μ A mean of a random value.

x A challenge.

y A response.

$y_i^{(t)}(x)$ The t-th response of the i-th PUF instance obtained by giving a challenge x.

5 Tests of PUFs

5.1 General

In this document, testing a PUF means verifying the security requirements defined in ISO/IEC 20897-1. As already mentioned in ISO/IEC 20897-1, for the purpose of the ISO/IEC 20897 series, the responses from multiple PUFs are arranged into a cube as shown in Figure 1. The repetitive calls to a PUF are illustrated in Figure 2. The single small cube describes a 1-bit response from a PUF. The three axes of the cube and the time are described hereafter, as directions:

— direction B: “#bits” shows the bit length of the response obtained from a single challenge. In a 1-bit response PUF, e.g., arbiter PUF, the dimension B collapses.

— direction C: “#challenges” shows the number of different challenges given to a PUF. In a no-challenge PUF (or, more rigorously, a one-challenge PUF), e.g., SRAM PUF[1], the dimension C collapses.

— direction D: “#PUF” shows the number of different PUF devices under test.

— direction T: “#query” shows the number of query iterations under the fixed PUF device and challenge.

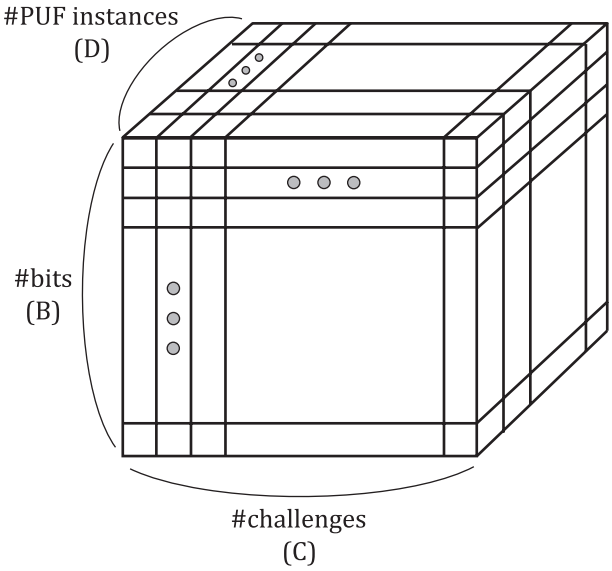

Figure 1 — Cube representation of the response sequences from multiple PUFs

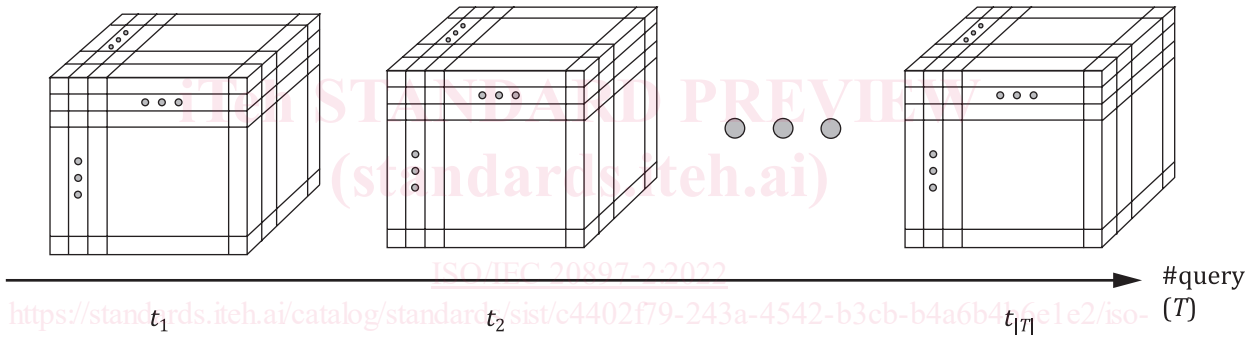

Figure 2 — Responses obtained by repetitive calls to the PUFs.

Among the defined security requirements, the steadiness, randomness and uniqueness may be tested by measuring responses from actual device(s) (Figures 1 and 2). If the empirical approaches are insufficient for evaluation, a stochastic model can be applied. If a stochastic model is used, the vendor shall provide the detailed document which explains the correctness of the model and the validity of the use of the model.

The tests based on stochastic models are defined in BSI AIS 31 standard and Reference [3]. They refer to an abstraction of the device where probabilistic aspects are clearly described. The model allows to derive ideal results, in terms of expectations over distributions (not only estimations based on limited sampling).

Notice that stochastic models shall be used in these two conditions:

— when a metric is not otherwise testable, owing to the prohibitive number of measurements which would be required,

— when a predictive (asymptotically) value of a metric is required.

For the stochastic model to be relevant, it shall rely on analogue random properties (such as delays, voltages, etc.). These measurements would typically be quantified to get the response bits. Some PUF structures may feature the capability to quantify the analogue properties, for example, when the response bits are obtained by a logical process. For instance, in the loop-PUF, the number of loops is counted. The response bit is subsequently computed based on a comparison between two (or more)

loop numbers. Thus, the information of the number of loops is available for analysis in a stochastic model.

Some PUF structures could add the capability of measurement quantification in a so-called "test mode." The quantification capability is thus intentionally added in an artificial manner for the sake of computing the metric. The addition of the quantification capability can be justified in situations where the PUF responses might be used only if the PUF itself is trusted.

5.2 Test conditions

The metrics shall be estimated according to several environmental conditions, including temperature, voltage, and humidity. Extreme values defined from the device standard operating conditions, e.g., the temperature and supply voltage specified in 7.7.4.3 of ISO/IEC 19790:2012, shall be tested. Also, some cycles between extreme values shall be performed, so as to check that the device is still functioning as intended. The accelerated aging techniques in Reference [5] may be used for this purpose.

5.3 Security tests

5.3.1 General

5.3 provides the concrete test and evaluation methods of a PUF. The security tests described in 5.3.2 through 5.3.7 corresponds to the security requirements defined in ISO/IEC 20897-1.

To claim that the PUF satisfies one or more of the security requirements, the vendor shall document the reason for that based on the conducted tests, evaluation results and/or design rationale. The document may include the logic diagram of the PUF building blocks, e.g., entropy source, entropy extractor, pre-processing block, post-processing block, and so forth. For the example of security requirements, evaluation criteria, and test conditions, see Annex D.

5.3.2 Test of steadiness

Steadiness is the repeatability over T measurements in Figure 2, that is, the estimation of a probability of failure based on repeated measurements. For devices which require a very high steadiness (e.g., for mission critical applications), the experimental approach can be insufficient in terms of error bars (estimation is too crude). In such a case, a stochastic model may be applied.

A PUF shall meet the steadiness requirement if the application of the PUF requires it (cf. 5.6, ISO/IEC 20897-1:2020). If a vendor claims that the PUF satisfies the steadiness requirement, the vendor shall document the reason for that. The steadiness shall be quantified by at least one metric: the intra-HD, bit error rate (BER), stochastic model, and so forth. The chosen value of challenge bits shall be precisely described, but is arbitrary. A vendor shall be responsible for determining the criterion of the steadiness considering the applications and operating environment of the PUF. It is the vendor's responsibility, if necessary, to check with the designer, manufacturer, and so forth for detailed information of the PUF in order to establish the evaluation criteria for steadiness. The concept of the test of steadiness is illustrated in Figure 3. For the example test procedure for steadiness, see Annex A.

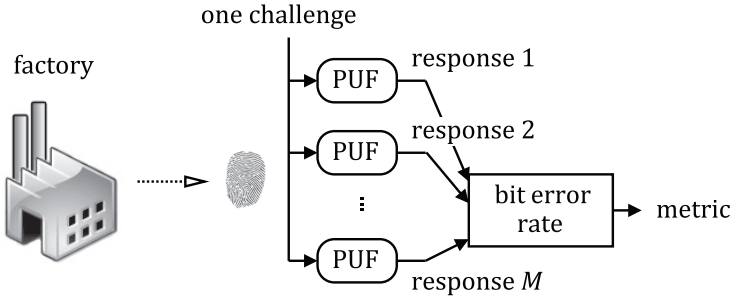

Figure 3 — Principle of the test for steadiness

5.3.3 Test of randomness

Randomness is the variability across B-C plane in Figure 1. A PUF shall meet the randomness requirement if the application of the PUF requires it (cf. 5.6, ISO/IEC 20897-1:2020). If a vendor claims that the PUF satisfies the randomness requirement, the vendor shall document the reason for that. A vendor shall be responsible for determining the criterion of the randomness considering the applications and operating environment of the PUF. It is the vendor's responsibility, if necessary, to check with the designer, manufacturer, and so forth for detailed information of the PUF in order to establish the evaluation criteria for randomness.

The randomness shall be tested by applying a statistical randomness test or entropy estimation to the B-C plain of the responses (see Figure 1). When the dimension C collapses (e.g., in confined PUFs), the test is applied to the bit sequence in dimension B. Similarly, when the dimension B collapses (e.g., in an arbiter PUF), the test is applied to the bit sequence in dimension C. Note that the randomness tests cannot apply to the cases without enough number of PUF responses. The tests may be the NIST FIPS 140-1[2], BSI AIS 31[3], SP800-22[6], SP800-90B[7] and so forth. The chosen value of challenge bits shall be precisely described, but is arbitrary. For the example test procedure for randomness, see Annex B.

NOTE FIPS 140-1 has been withdrawn, but that its entropy tests are still reliable methods which can be repurposed to evaluate a PUF.

5.3.4 Test of uniqueness

Uniqueness is the variability across B-D plane in Figure 1. A PUF shall meet the uniqueness requirement if the application of the PUF requires it (cf. 5.6, ISO/IEC 20897-1:2020). If a vendor claims that the PUF satisfies the uniqueness requirement, the vendor shall document the reason for that. A vendor shall be responsible for determining the criterion of the uniqueness considering the applications and operating environment of the PUF. It is the vendor's responsibility, if necessary, to check with the designer, manufacturer, and so forth for detailed information of the PUF in order to establish the evaluation criteria for uniqueness.

The uniqueness shall be assessed by evaluating the inter-Hamming distance of the responses among the PUF devices, or by the statistical ways similar to the randomness. In practice, it is not always possible to prepare a sufficient number of devices for the test of uniqueness. In such a case, a stochastic model may leverage the test (see C.4). If the uniqueness is evaluated by the statistical tests, the applicable test includes the NRBG health test in ISO/IEC 18031:2011[8] which is based on FIPS 140-1[2] and AIS-31[3], and NIST SP800-90B[7]. The concept of the test of uniqueness is illustrated in Figure 4. The chosen value of challenge bits shall be precisely described, but is arbitrary. For the example test procedure for uniqueness, see Annexes B and C.

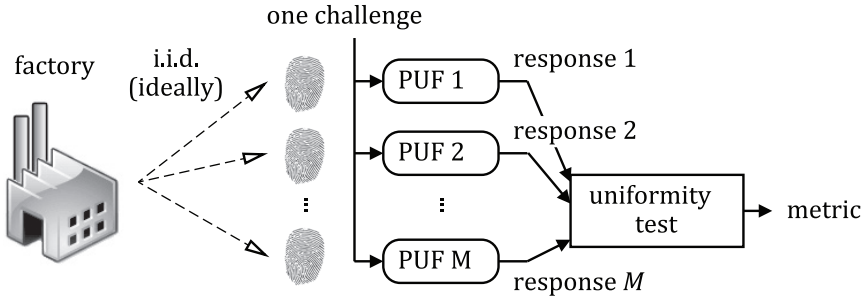

Figure 4 — Test of uniqueness

5.3.5 Test of Tamper-resistance

The test of the tamper-resistance verifies whether the PUF does not leak secret data nor lose requisite properties by invasive, semi-invasive and non-invasive physical attacks. The examples of the physical attacks include side-channel attacks, reverse engineering, using fault analysis tools such as LVP and FIB.

A PUF shall meet the tamper-resistance requirement if the application of the PUF requires it (cf. 5.6, ISO/IEC 20897-1:2020). If a vendor claims that the PUF satisfies the tamper-resistance requirement, the vendor shall document the reason for that. A PUF vendor shall be responsible for adducing the rationale for the tamper-resistance based on the conducted tests, evaluation results, design and implementation of the PUF. It is the vendor's responsibility, if necessary, to check with the designer, manufacturer, and so forth for detailed information of the PUF in order to establish the evaluation criteria for tamper-resistance.

5.3.6 Test of Mathematical unclonability

The test of the mathematical unclonability verifies whether the PUF's challenge-response behaviour is not simulated or emulated by other devices. A mathematically unclonable PUF generates responses which are difficult to be corelated to the challenge, design and implementation of the PUF. A PUF is mathematically unclonable if it is impossible to disclose the mapping table or function of the CRPs by for example dictionary attacks, machine learning attacks, and so on.

A PUF shall meet the mathematical unclonability if the application of the PUF requires it (cf. 5.6, ISO/IEC 20897-1:2020). If a vendor claims that the PUF satisfies the mathematical unclonability, the vendor shall document the reason for that. A PUF vendor shall be responsible for adducing the rationale for the mathematical unclonability based on the conducted tests, evaluation results, design and implementation of the PUF. It is the vendor's responsibility, if necessary, to check with the designer, manufacturer, and so forth for detailed information of the PUF in order to establish the evaluation criteria for mathematical unclonability.

5.3.7 Test of Physical unclonability

The test of the physical unclonability verifies whether the physical clone of the PUF is impractical to be manufactured. The physical unclonability ensures that there are no two PUFs that have the same input-output behaviour. The physical unclonability is assessed by examining whether the PUF surely utilizes the entropy source derived from the uncontrollable device variation.

A PUF shall meet the physical unclonability if the application of the PUF requires it (cf. 5.6, ISO/IEC 20897-1:2020). If a vendor claims that the PUF satisfies the physical unclonability, the vendor shall document the reason for that. A PUF vendor shall be responsible for adducing the rationale for the physical unclonability based on the conducted tests, evaluation results, design or implementation of the PUF. It is the vendor's responsibility, if necessary, to check with the designer, manufacturer, and so forth for detailed information of the PUF in order to establish the evaluation criteria for physical unclonability.