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 IID	Independent and identically distributed.
NRBG	Non-deterministic random bit generator