INTERNATIONAL STANDARD

ISO/IEC 20543

First edition
2019-10

Information technology — Security techniques — Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408

Technologies de l'information — Techniques de sécurité — Méthodes d'essai et d'analyse des générateurs de bits aléatoires dans l'ISO/IEC 19790 et l'ISO/IEC 15408

Reference number
ISO/IEC 20543:2019(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, *IT security techniques*.

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 applications need random numbers for a wide range of tasks. A strong cryptographic random bit generator that is suitable for general cryptographic applications is expected to provide output bit strings that cannot be distinguished with any potentially practical computational effort and any potentially practical sample sizes from bit strings of the same length drawn uniformly at random. Furthermore, such an RBG is expected to offer enhanced backward secrecy and enhanced forward secrecy.

Information technology — Security techniques — Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408

1 Scope

This document specifies a methodology for the evaluation of non-deterministic or deterministic random bit generators intended to be used for cryptographic applications. The provisions given in this document enable the vendor of an RBG to submit well-defined claims of security to an evaluation authority and shall enable an evaluator or a tester, for instance a validation authority, to evaluate, test, certify or reject these claims.

This document is implementation-agnostic. Hence, it offers no specific guidance on design and implementation decisions for random bit generators. However, design and implementation issues influence the evaluation of an RBG in this document, for instance because it requires the use of a stochastic model of the random source and because any such model is supported by technical arguments pertaining to the design of the device at hand.

Random bit generators as evaluated in this document aim to output bit strings that appear evenly distributed. Depending on the distribution of random numbers required by the consuming application, however, it is worth noting that additional steps can be necessary (and can well be critical to security) for the consuming application to transform the random bit strings produced by the RBG into random numbers of a distribution suitable to the application requirements. Such subsequent transformations are outside the scope of evaluations performed in this document.

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 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

ISO/IEC 17825, *Information technology — Security techniques — Testing methods for the mitigation of non-invasive attack classes against cryptographic modules*

ISO/IEC 18031:2011, *Information technology — Security techniques — Random bit generation*

ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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
backward secrecy
assurance that previous RBG output values cannot be determined from knowledge of current or subsequent output values

3.2
bit stream
continuous output of bits from a device or mechanism

[SOURCE: ISO/IEC 18031:2011, 3.4]

3.3
black box
idealized mechanism that accepts inputs and produces outputs, but is designed such that an observer cannot see inside the box or determine exactly what is happening inside that box

Note 1 to entry: This term can be contrasted with *glass box* (3.13).

[SOURCE: ISO/IEC 18031:2011, 3.6]

3.4
conformance-tester
tester
individual assigned to perform test activities in accordance with a given conformance testing standard and associated testing methodology

EXAMPLE An example of such a standard is ISO/IEC 19790 and the testing methodology specified in ISO/IEC 24759.

[SOURCE: ISO/IEC 19896-1:2018, 3.2, modified — The term "tester" has been added as an admitted term.]

3.5
deterministic random bit generator
DRBG
random bit generator that produces a random-appearing sequence of bits by applying a deterministic algorithm to a suitably random initial value called a seed and, possibly, some secondary inputs

Note 1 to entry: Non-deterministic sources can also form part of these secondary inputs.

Note 2 to entry: The security of a deterministic random bit generator rests primarily on the strength of its cryptographic algorithms and on the randomness contained in the seed value. In a deterministic random bit generator that is suitable for cryptographic use, at least forward and backward secrecy shall be assured without invoking secondary inputs to the RBG or reseeding."

3.6
enhanced backward secrecy
assurance that the knowledge of the current internal state of a random bit generator does not allow an adversary to derive with practical computational effort knowledge about previous output values

Note 1 to entry: The notion of enhanced backward secrecy is trivial for memoryless RBGs. Therefore, it is only a useful notion for deterministic and hybrid RBGs, the security of which rests at least in part on cryptographic properties of the state transition function and the output generation function of the random bit generator.

3.7
enhanced forward secrecy
assurance that knowing the current internal state of the random bit generator does not yield practically relevant constraints on subsequent (future) output values

Note 1 to entry: Deterministic random bit generators are unable to achieve enhanced forward secrecy. Unlike forward and backward secrecy as well as enhanced backward secrecy, enhanced forward secrecy rests entirely on the ability of a continuous reseeding process to supply as much entropy as is required to make the prediction of future outputs infeasible.

Note 2 to entry: It is possible for a random bit generator to have enhanced forward secrecy but still expand entropy, i.e. output a bit-string that can in principle be significantly compressed". For instance, one can consider an RBG design with a random source which produces at each invocation a 128 bit random string *R* with an estimated 120 bits of min entropy, with a 512 bit internal state *S(n)*, a state transition function giving *S(n+1) := SHA3-512(S(n)||R)*, and an output generation function applying SHAKE-256 on *S(n)||R* with up to 1024 bits of output per invocation.

Note 3 to entry: Another term often found in the literature that is interchangeable with enhanced forward secrecy is prediction resistance.

3.8
entropy
measure of the expected amount of information contained in a bit string given knowledge of how the bit string was generated

Note 1 to entry: There are various notions of entropy that play a role in cryptography. Worth mentioning among them are Shannon entropy, min entropy, collision entropy, guessing entropy, algorithmic entropy and Renyi entropy (the latter notion containing as special cases among others Shannon entropy, Min entropy and Collision entropy).

Note 2 to entry: The amount of entropy contained in an unknown bit string is always relative to an observer. RBG evaluations establish entropy estimates in face of an attacker with detailed knowledge about the entropy source and also consider her abilities to observe or influence the state of the entropy source.

Note 3 to entry: Irrespective of the chosen kind of entropy, the term "full entropy" always means the same, namely uniformly distributed and independent random numbers, that is, ideal randomness.

Note 4 to entry: An algorithmic entropy is a logarithm to the base 2 of the length of the shortest encoding in some given formal language. Its measure is based on the notion of optimal compression. The algorithmic entropy of a bit-string is dependent on the underlying formal language and even given a well-defined formal language, is in general incomputable unless the language is very restricted. However, related notions are of relevance in a cryptographic context. For instance, one can ask how much the sequence of raw random numbers derived from some physical noise source can be compressed using some fixed computationally efficient compression strategy that is informed by a precise understanding of the physical noise source and of the process that converts the output of the noise source into the raw random numbers.

3.9
entropy source
mechanism or device which produces intrinsically unpredictable output

Note 1 to entry: In the context of purely deterministic random bit generators, entropy generation can be performed just once, and in this case, it is possible for the RBG device not to contain an entropy source. The source of the entropy used by such an RBG nevertheless needs to be evaluated to the same standards that would otherwise be required.

Note 2 to entry: In some circumstances, it can be admissible for a deterministic RBG to be seeded with externally generated entropy instead of containing hardware that produces entropy within its own perimeter. In that case, the externally generated entropy shall only be available to the RBG instance it is intended for.

3.10
evaluator
individual assigned to perform evaluations in accordance with a given evaluation standard and associated evaluation methodology

Note 1 to entry: An example of an evaluation standard is ISO/IEC 15408 (all parts) with the associated evaluation methodology given in ISO/IEC 18045.

[SOURCE: ISO/IEC 19896-1:2018, 3.5]

3.11
forward secrecy
assurance that the knowledge of subsequent (future) values cannot be determined from current or previous values

[SOURCE: ISO/IEC 18031:2011, 3.13]

3.12
glass box
idealized mechanism that accepts inputs and produces outputs and is designed such that an observer can see inside and determine exactly what is going on

Note 1 to entry: This term can be contrasted with *black box* (3.3).

[SOURCE: ISO/IEC 18367:2016, 3.12]

3.13
health test
online test and total failure test
any mechanism (statistical test or otherwise) which detects at least one of the following two scenarios:

a) a transient or permanent total failure of the entropy source, i.e. a drastic decrease in entropy which usually manifests itself in a small number of easily detectable symptoms

b) smaller deviations from the normal behaviour of the entropy source, but nevertheless intolerable which undermine security claims made by the vendor. In contrast to a total failure, it usually requires a slightly larger sample size until these deviations are reliably detected

3.14
independent and identically distributed
IID

property of a family of random variables stating that they share the same distribution and are mutually independent

3.15
laboratory
organization with a management system providing evaluation and or testing work in accordance with a defined set of policies and procedures and utilizing a defined methodology for testing or evaluating the security functionality of IT products

Note 1 to entry: These organizations are often given alternative names by various approval authorities. For example, IT Security Evaluation Facility (ITSEF), Common Criteria Testing Laboratory (CCTL), Commercial Evaluation Facility (CLEF).

[SOURCE: ISO/IEC 19896-1:2018, 3.8]

3.16
min entropy
the min entropy of a finite random variable *X is –log2(p_max)* where *p_max* denotes the probability of the most likely outcome. That is, *p_max >=p_x* for all *x*

3.17
guessing entropy
guess work
<of *X*> expected number of guesses an adversary following an optimal guessing strategy needs to submit in order to guess the value of *x*[19], with *X*, a random finite variable and *x*, the value of a realization of *X* (i.e. a corresponding random variate)

Note 1 to entry: The formula for the guessing entropy is *\sum_i=1^n ip_i* where the *p_i* are ordered *p_1 >= p_2 >= ...* (that is, the optimal guessing strategy is to guess the most likely outcomes first).

3.18
non-dedicated non-deterministic random bit generator
NNRBG
non-deterministic random bit generator the security of which is not based on randomness generated by hardware that was designed explicitly to generate randomness

Note 1 to entry: TNRBG und NNRBG stand for true dedicated NRBG and non-dedicated NRBG, respectively.

3.19
non-deterministic random bit generator
NRBG
random bit generator that continuously samples multiple entropy sources and, if operating correctly, has an output that is expected to be unpredictable for attackers with unbounded computational capabilities over short timescales

3.20
perfect forward secrecy
property of a cryptographic protocol whereby an attacker cannot compromise past runs of the protocol by learning the long-term secrets of the participants

3.21
physical entropy source
entropy source based on the use of a dedicated physical effect (e.g. noisy diode, nuclear decay, etc.)

3.22
noise source
element of a technical system or its environment which produces partially unpredictable output. In this document, "noise source" and "entropy source" are taken to be entropy sources

3.23
non-physical entropy source
entropy source not based on a dedicated physical system but on unpredictable parts of the environment or technical components that were not originally designed for random bit generation

Note 1 to entry: Examples can be user input or the collection of various difficult to predict system data (e.g. hard drive access times, noise from a sensor device, system interrupts) in a standard computer.

3.24
post-processing
part of a random bit generator which processes the output of a random source with the aim of removing dependencies between random bits or biases. Is often also referred as a conditioning component

3.25
random bit generator
RBG
device or algorithm designed to produce bits that appear statistically independent and unbiased

Note 1 to entry: In case of purely physical random bit generators, the existence of very small entropy defects can be permitted. Deterministic RBG constructions, on the other hand, shall offer output that is computationally indistinguishable in practice from ideally distributed data. In addition, it is worth noting that hybrid designs have advantages over both purely deterministic and purely physical designs by combining the true entropy guarantees of physical RBGs with the near-ideal output distribution of deterministic RBGs and resilience properties, for instance with regards to noise source failure.

3.26
raw random numbers
bit sequence produced internally within a random bit generator by digitization of the random noise source or detection of unpredictable events within the machine in question, before any post-processing beyond the digitization has been performed

Note 1 to entry: It should be noted that although the raw random numbers represent an early stage in random bit generation, they can already contain complicated inherent pseudo-random patterns. For instance, part of the randomness in hard drive seek times is commonly associated to chaotic turbulent air flow patterns inside the hard drive; even if one abstracts away all other features of a hard drive, it seems difficult to argue that an RBG based on this effect does not have significant internal memory. However, sources with large internal memory are notoriously difficult to properly characterise by statistical tests with realistic sample sizes. The extent to which pseudorandom patterns are exhibited by a raw random source therefore depends on the design of the entropy source and shall be considered when analysing it. Generic statistical tests can mistake pseudo-randomness for actual randomness and thus overestimate the entropy of the raw random numbers. It is for this reason primarily that it is important to understand the design of the mechanism producing the raw random numbers. This comprises influences of the digitization mechanisms itself, e.g. resolution and non-linearity of A/D converters or noise produced by amplification circuits.

3.27
security strength
largest natural number, *n*, such that a computationally unbounded attacker cannot distinguish with more than negligible advantage an *n*-bit value produced by the RBG from an *n*-bit value drawn uniformly at random, when given the true prior distribution of internal RBG states

Note 1 to entry: If no such number *n* exists, the security strength is said to be infinite.

Note 2 to entry: Only hybrid or physical random bit generators can have infinite maximal supported security strength, as deterministic random bit generators always rely on an initial seed value. It is worth noting, however, that the output of pure physical random bit generators can often be distinguished from random data in practice if the design of any conditioning steps that can be performed is known to the attacker.

3.28
Shannon entropy
<of a finite random variable *X*> expected value of *–log2(px),* where *px* is the probability of observing the realization *X=x*

Note 1 to entry: In other words, for a finite random variable *X* with range *S* that the Shannon entropy *H(X)* is given by the formula $H(X) = -\sum x \in S \cdot px \cdot log2(px)$, where for the purposes of calculating the expected value one adopts the convention that *0*log2(0) = 0*.

3.29
stationarity
property of a stochastic process whereby the joint distribution of subsequent instances of the process is time-invariant

3.30
stochastic model
partial mathematical description of a random bit generator based on at least a qualitative understanding of the entropy source which, together with possibly some data gathered empirically for parameter estimation, allows the derivation of entropy claims

Note 1 to entry: In the context of evaluating random bit generators, it is recommended but not required that the stochastic model describe the behaviour of the raw random bits. Subsequent post-processing can make it more difficult to make a convincing case that the stochastic model is in sufficient correspondence with the workings of the device to be modelled to support the entropy claims to be shown. For instance, a stochastic model applied to the output random numbers of a deterministic random bit generator will be essentially untestable statistically insofar as strong cryptographic post-processing can render even very low entropy data indistinguishable from random noise at realistic sample sizes, at least from the point of view of any adversary lacking a stochastic model of the raw random numbers.

3.31
TNRBG
non-deterministic random bit generator the security of which is based on a hardware component that has been designed explicitly to generate randomness

Note 1 to entry: TNRBG und NNRBG stand for true dedicated NRBG and non-dedicated NRBG, respectively.

3.32
validation authority
entity that will validate the testing results for conformance to ISO/IEC 19790

[SOURCE: ISO/IEC 19790:2012, 3.132, modified — In the definition, "this International Standard" has been changed to "ISO/IEC 19790".]

3.33
vendor
entity, group or association that submits the cryptographic module for testing and validation

Note 1 to entry: The vendor has access to all relevant documentation and design evidence regardless if they did or did not design or develop the cryptographic module.

[SOURCE: ISO/IEC 19790:2012, 3.133]

4 Symbols and abbreviated terms

CCTL	Common Criteria Testing Laboratory
CLEF	Commercial Evaluation Facility
ITSEF	IT Security Evaluation Facility
LFSR	Linear Feedback Shift Register
OS	Operating System
SHA	Secure Hash Algorithm (SHA-256 and SHA3-512 referred to in this document)

5 Structure of this document

This document is divided into five clauses after the current clause: overview of non-deterministic random bit generators, conformance testing of NRBG, overview of deterministic random bit generator, conformance testing of DRBG and testing methodology. Each clause focuses on testing and evaluation activities for random bit generators for a conformance scheme using ISO/IEC 19790 and an evaluation scheme using the ISO/IEC 15408 series.

6 Overview of non-deterministic random bit generators

6.1 Introductory remarks on random bit generation

The current clause intends to demonstrate the problems of evaluating random bit generators and the security goals that are to be achieved by looking at the well-known setting of coin-tossing. One side of the coin is called "a head" (H) and the other is called "a tail" (T). Randomness is generated by tossing the coin into the air and noting which side is up when it lands.

Flipping a coin multiple times produces an ordered series of coin flip results denoted as a series of $H(s)$ and $T(s)$. For example, the sequence "*HTTHT*" (reading left to right) indicates a head followed by a tail, followed by a tail, followed by a head, followed by a tail. This coin flip sequence can be translated into