
**Information technology — Security
techniques — Random bit generation**

*Technologies de l'information — Techniques de sécurité — Génération
de bits aléatoires*

**iTeh STANDARD PREVIEW
(standards.iteh.ai)**

[ISO/IEC 18031:2005](https://standards.iteh.ai/catalog/standards/sist/f7d90a10-40fe-4e7d-88d8-01a4faad0058/iso-iec-18031-2005)

<https://standards.iteh.ai/catalog/standards/sist/f7d90a10-40fe-4e7d-88d8-01a4faad0058/iso-iec-18031-2005>

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 18031:2005](#)

<https://standards.iteh.ai/catalog/standards/sist/f7d90a10-40fe-4e7d-88d8-01a4faad0058/iso-iec-18031-2005>

© ISO/IEC 2005

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword.....	vi
Introduction	vii
1 Scope	1
2 Normative references	1
3 Terms and definitions.....	2
4 Symbols	5
5 Overarching objectives and requirements of a random bit generator.....	5
5.1 Required properties of randomness.....	6
5.2 Backward and forward secrecy.....	6
5.3 Top-level objectives and requirements for a random bit generator (RBG) output.....	7
5.4 Top-level objectives and requirements for RBG operation.....	7
5.5 Random bit generator functional requirements	8
6 General functional model for random bit generation.....	8
6.1 Basic components.....	8
6.1.1 Entropy source.....	9
6.1.2 Additional inputs.....	10
6.1.3 Internal state.....	10
6.1.4 Internal state transition functions.....	11
6.1.5 Output generation function	12
6.1.6 Support functions.....	13
7 Types of random bit generators.....	14
7.1 Non-deterministic random bit generators (NRBGs).....	14
7.2 Deterministic random bit generators (DRBGs).....	15
7.3 The RBG spectrum	15
8 Overview and requirements for a non-deterministic random bit generator.....	16
8.1 Overview	16
8.2 Functional model of a non-deterministic random bit generator.....	16
8.2.1 Overview of the model.....	16
8.3 Entropy sources.....	18
8.3.1 Primary entropy source	18
8.3.2 Physical entropy sources	20
8.3.3 Non-physical entropy sources	21
8.3.4 Additional entropy sources	21
8.3.5 Hybrid non-deterministic random bit generators	22
8.4 Additional inputs.....	23
8.4.1 Overview	23
8.4.2 Mandatory requirements.....	23
8.5 Internal state.....	23
8.5.1 Overview	23
8.5.2 Mandatory requirements	24
8.5.3 Optional requirements.....	24
8.6 Internal state transition functions.....	25
8.6.1 Overview	25
8.6.2 Mandatory requirements.....	26
8.6.3 Optional requirements.....	26
8.7 Output generation function	26
8.7.1 Overview	26
8.7.2 Mandatory requirements.....	26

8.7.3	Optional requirement	27
8.8	Health tests	27
8.8.1	Overview	27
8.8.2	General health test requirements	27
8.8.3	Health test on deterministic components	28
8.8.4	Health tests on entropy sources	28
8.8.5	Health tests on random output	29
8.9	Component interaction	31
8.9.1	Overview	31
8.9.2	Mandatory requirements	31
8.9.3	Optional requirements	32
9	Overview and requirements for a deterministic random bit generator	32
9.1	Overview	32
9.2	Functional model of DRBG	33
9.2.1	Overview of the model	33
9.3	Entropy source	35
9.3.1	Primary entropy source	35
9.3.2	Generating seed values	37
9.3.3	Additional entropy sources	37
9.3.4	Hybrid deterministic random bit generator	38
9.4	Additional inputs	38
9.5	Internal state	38
9.6	Internal state transition function	39
9.7	Output generation function	40
9.7.1	Overview	40
9.8	Support functions	40
9.8.1	Overview	40
9.8.2	Self test	40
9.8.3	Deterministic algorithm test	41
9.8.4	Software/Firmware integrity test	41
9.8.5	Critical functions test	41
9.8.6	Software/Firmware load test	41
9.8.7	Manual key entry test	41
9.8.8	Continuous random bit generator test	42
9.9	Additional DRBG functional requirements	42
9.9.1	Keys	42
Annex A (normative) Combining random bit generators		44
Annex B (normative) Conversion methods		45
B.1	Random number generation	45
B.1.1	The simple discard method	45
B.1.2	The complex discard method	45
B.1.3	The simple modular method	46
B.1.4	The complex modular method	46
B.2	Extracting bits in the Dual_EC_DRBG	47
B.2.1	Potential bias in an elliptic curve over a prime field F_p	47
B.2.2	Adjusting for the missing bit(s) of entropy in the x coordinates	48
B.2.3	Values for E	49
B.2.4	Observations	51
Annex C (normative) Deterministic random bit generators		52
C.1	Introduction	52
C.2	Deterministic RBGs based on a hash-function	52
C.2.1	Hash-function DRBG (Hash_DRBG)	52
C.3	DRBG based on block ciphers	60
C.3.1	CTR_DRBG	61
C.3.2	OFB_DRBG (...)	70
C.4	Deterministic RBGs based on number theoretic problems	72
C.4.1	Dual Elliptic Curve DRBG (Dual_EC_DRBG)	72
C.4.2	Micali Schnorr DRBG (MS_DRBG)	81

Annex D (normative) Application specific constants	91
D.1 Constants for the Dual_EC_DRBG	91
D.1.1 Curves over Prime Fields	91
D.1.2 Curves over binary fields	94
D.2 Default moduli for the MS_DRBG (...)	103
D.2.1 Default modulus n of size 1024 bits	103
D.2.2 Default modulus n of size 2048 bits	103
D.2.3 Default modulus n of size 3072 bits	104
D.2.4 Default modulus n of size 7680 bits	104
D.2.5 Default modulus n of size 15360 bits	105
Annex E (informative) Non-deterministic random bit generator examples	107
E.1 Canonical coin tossing example	107
E.1.1 Overview	107
E.1.2 Description of basic process	107
E.1.3 Relation to standard NRBG components	107
E.1.4 Optional variations	108
E.1.5 Peres unbiasing procedure	108
E.2 Hypothetical noisy diode example	109
E.2.1 Overview	109
E.2.2 General structure	109
E.2.3 Details of operation	110
E.2.4 Failsafe design consequences	114
E.2.5 Modified example	114
E.3 Mouse movement example	115
Annex F (informative) Security considerations	116
F.1 Attack model	116
F.2 The security of hash-functions	116
F.3 Algorithm and key size selection	116
F.3.1 Equivalent algorithm strengths	117
F.3.2 Selection of appropriate DRBGs	118
F.4 The security of block cipher DRBGs	119
F.5 Conditioned entropy sources and the derivation function	119
Annex G (informative) Discussion on the estimation of entropy	120
Annex H (informative) Random bit generator assurance	121
Annex I (informative) Random bit generator boundaries	122
Bibliography	124

Foreword

ISO (the International Organization for Standardization) and IEC (International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO and 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 18031 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

PRE-STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 18031:2005](https://standards.iteh.ai/catalog/standards/sist/f7d90a10-40fe-4e7d-88d8-01a4faad0058/iso-iec-18031-2005)

<https://standards.iteh.ai/catalog/standards/sist/f7d90a10-40fe-4e7d-88d8-01a4faad0058/iso-iec-18031-2005>

Introduction

This International Standard sets out specific requirements that when met will result in the development of a random bit generator that may be applicable to cryptographic applications.

Numerous cryptographic applications require the use of random bits. These cryptographic applications include the following:

- random keys and initialisation values (IVs) for encryption;
- random keys for keyed MAC algorithms;
- random private keys for digital signature algorithms;
- random values to be used in entity authentication mechanisms;
- random values to be used in key establishment protocols;
- random PIN and password generation;
- nonces.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

The purpose of this International Standard is to establish a conceptual model, terminology, and requirements related to the building blocks and properties of systems used for random bit generation in or for cryptographic applications.

[ISO/IEC 18031:2005](https://standards.iteh.ai/catalog/standards/sist/f7d90a10-40fe-4e7d-88d8-)

<https://standards.iteh.ai/catalog/standards/sist/f7d90a10-40fe-4e7d-88d8->

In general terms, it is possible to categorize random bit generators into two types depending on whether their source of entropy varies or is fixed. This International Standard identifies the two types as non-deterministic and deterministic random bit generators.

A non-deterministic random bit generator can be defined as a random bit generating mechanism that uses a source of entropy to generate a random bit stream.

A deterministic random bit generator can be defined as a bit generating mechanism that uses deterministic mechanisms, such as cryptographic algorithms on a source of entropy, to generate a random bit stream. In this type of bit stream generation, there is a specific input (normally called a seed) and perhaps some optional input, which, depending on its application may or may not be publicly available. The seed is processed by a function which provides an output.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 18031:2005](#)

<https://standards.iteh.ai/catalog/standards/sist/f7d90a10-40fe-4e7d-88d8-01a4faad0058/iso-iec-18031-2005>

Information technology — Security techniques — Random bit generation

1 Scope

This International Standard specifies a conceptual model for a random bit generator for cryptographic purposes, together with the elements of this model.

This International Standard also includes the following:

- the description of the main elements required for a non-deterministic random bit generator;
- the description of the main elements required for a deterministic random bit generator;
- their characteristics;
- their security requirements.

Where there is a requirement to produce sequences of random numbers from random bit strings, Annex B provides guidance on how this can be performed.

Techniques for statistical testing of random bit generators for the purposes of independent verification or validation, and detailed designs for such generators, are outside the scope of this International Standard.

2 Normative references

The following referenced documents are indispensable for the application 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 10116, *Information technology — Security techniques — Modes of operation for an n -bit block cipher*

ISO/IEC 10118-3:2004, *Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

ISO/IEC 18032:2004, *Information technology — Security techniques — Prime number generation*

ISO/IEC 18033-3:2005, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*¹⁾

1) To be published.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1 algorithm
clearly specified mathematical process for computation; a set of rules that, if followed, will give a prescribed result.

3.2 backward secrecy
assurance that previous values cannot be determined from the current value or subsequent values.

3.3 biased source
source of bit strings (or numbers) from a sample space is said to be biased if some bit string(s) (or number(s)) are more likely than some other bit string(s) (or number(s)) to be chosen. Equivalently, if the sample space consists of r elements, some elements will occur with probability different from $1/r$.

cf. **unbiased source**

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

3.5 bit string
finite sequence of ones and zeros.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.6 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.

cf. **glass box**

3.7 block cipher
symmetric encipherment system with the property that the encryption operates on a block of plaintext, i.e., a string of bits of a defined length, to yield a block of ciphertext. [ISO/IEC 18033-1]

3.8 cryptographic boundary
explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software and/or firmware components of a cryptographic module. [ISO/IEC 19790]

3.9 deterministic algorithm
characteristic of an algorithm that states that given the same input, the same output is always produced.

3.10 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 upon which the security of the random bit generator does not depend. In particular, non-deterministic sources may also form part of these secondary inputs.

3.11**entropy**

measure of the disorder, randomness or variability in a closed system. The entropy of X is a mathematical measure of the amount of information provided by an observation of X .

3.12**entropy source**

component, device or event which produces outputs which, when captured and processed in some way, produces a bit string containing entropy.

3.13**forward secrecy**

assurance that subsequent (future) values cannot be determined from current or previous values.

3.14**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.

cf. **black box**

3.15**hash-function**

function, which maps strings of bits to fixed-length, strings of bits, satisfying the following two properties.

- It is computationally infeasible to find for a given output, an input that maps to this output.
- It is computationally infeasible to find for a given input, a second input, which maps to the same output.

NOTE Computational feasibility depends on the specific security requirements and environment. [ISO/IEC 10118-1]

3.16**human entropy source**

entropy source that has some kind of random human component.

3.17**hybrid deterministic random bit generator (Hybrid DRBG)**

DRBG is said to be a "hybrid" DRBG if it uses a non-deterministic entropy source as an additional entropy source.

3.18**hybrid non-deterministic random bit generator****Hybrid NRBG**

(physical or non-physical) NRBG is said to be a "hybrid" NRBG if it takes a seed value as an additional entropy source.

3.19**initialisation value**

value used in defining the starting point of a cryptographic algorithm (e.g., a hash-function or an encryption algorithm).

3.20**Kerckhoffs box**

idealized cryptosystem where the design and public keys are known to an adversary, but in which there are secret keys and/or other private information that is not known to an adversary. A Kerckhoffs Box lies between a black box and a glass box in terms of the knowledge of an adversary.

3.21

known-answer test

method of testing a deterministic mechanism where a given input is processed by the mechanism and the resulting output is then compared to a corresponding known value.

NOTE Known Answer Testing of a deterministic mechanism may also include testing the integrity of the software which implements the deterministic mechanism. For example, if the software implementing the deterministic mechanism is digitally signed, the signature can be recalculated, and compared to the known signature value.

3.22

min-entropy

bit string X has min-entropy k if k is the largest value such that $\Pr [X = x] \leq 2^{-k}$. That is, X contains k bits of min-entropy or randomness.

NOTE Informally, this is the "best" kind of entropy.

3.23

non-deterministic random bit generator

NRBG

RBG whose security depends upon sampling an entropy source. The entropy source shall be sampled whenever the RBG produces output, and possibly more often.

3.24

one-way function

function with the property that it is easy to compute the output for a given input but it is computationally infeasible to find for a given output an input, which maps to this output. [ISO/IEC 11770-3]

ITIH STANDARD PREVIEW

(standards.iteh.ai)

3.25

output generation function

function in a random bit generator that outputs bits that appear to be random.

[ISO/IEC 18031:2005](https://standards.iteh.ai/catalog/standards/sist/f7d90a10-40fe-4e7d-88d8-01a4faad0058/iso-iec-18031-2005)

3.26

pseudorandom sequence

sequence of bits or a number is pseudorandom if it appears to be selected at random even though the selection process is done by a deterministic algorithm.

<https://standards.iteh.ai/catalog/standards/sist/f7d90a10-40fe-4e7d-88d8-01a4faad0058/iso-iec-18031-2005>

3.27

pure deterministic random bit generator

DRBG is said to be a "pure" DRBG if all of its entropy sources are seeds.

3.28

pure non-deterministic random bit generator

(physical or non-physical) NRBG is said to be a "pure" NRBG if all of its entropy sources are non-deterministic.

3.29

random bit generator

RBG

device or algorithm that outputs a sequence of bits that appears to be statistically independent and unbiased.

3.30

reseeding

specialized internal state transition function which updates the internal state in the event that a new seed value is supplied.

3.31

secret parameter

input to the RBG during initialisation. It provides additional entropy in the case of an entropy source failure or compromise.

3.32**seed**

string of bits that is used as input to a deterministic random bit generator (DRBG). The seed will determine a portion of the state of the DRBG.

3.33**seedlife**

period of time between initialising the DRBG with one seed and reseeding (fully initialising) that DRBG with another seed.

3.34**state**

state is defined as a condition of a random bit generator or any part thereof with respect to time and circumstance.

3.35**unbiased source**

source of bit strings (or numbers) from a sample space is said to be unbiased if all potential bit strings (or numbers) have the same possibility of being chosen. Equivalently, if the sample space consists of r elements, all elements will occur with probability $1/r$.


cf. **biased source**

4 Symbols**iTeh STANDARD PREVIEW**

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

(standards.itih.ai)

Symbol**Meaning**

Symbol	Meaning
$\text{Pr}[x]$	Probability of x . <small>https://standards.iso.org/standards/sist/f7d90a10-40fe-4e7d-88d8-01a4faad0058/iso-iec-18031-2005</small>
IV	Initialisation Value.
$\lceil X \rceil$	Ceiling: the smallest integer greater than or equal to X . For example, $\lceil 5 \rceil = 5$, and $\lceil 5.3 \rceil = 6$.
$X \oplus Y$	Bitwise exclusive-or (also bit wise addition mod 2) of two bit strings X and Y of the same length.
$X \parallel Y$	Concatenation of two strings X and Y in that order. X and Y are either both bit strings, or both octet strings.
$ a $	The length in bits of string a .
$x \bmod n$	The unique remainder r , $0 \leq r \leq n-1$, when integer x is divided by n . For example, $23 \bmod 7 = 2$.
	Used in a figure to illustrate a "switch" between sources of input.

5 Overarching objectives and requirements of a random bit generator

The properties of randomness may be demonstrated by tossing a coin in the air and observing which side is uppermost when it lands, where one side is called "heads" (H) and the opposite is called "tails" (T). A coin also has a rim, but the probability that a coin might land on its rim is so unlikely an occurrence that for the purpose of this demonstration it may be ignored.

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 a binary string in a straightforward manner by assigning H to a binary one ('1') and T to a binary zero ('0'); the resulting example bit string is '10010'.

5.1 Required properties of randomness

The required properties of randomness can be examined using the example of the idealized coin toss described above. The result of each coin flip is:

1. Unpredictable: Before the flip, it is unknown whether the coin will land on heads or tails. Also, if that flip is kept secret, it is not possible to determine what the flip was if any subsequent flip outcome is known. The unpredictability after the flip depends on whether the observer can observe the coin flip or not. The notion of entropy quantifies the amount of unpredictability or uncertainty relative to an observer and will be discussed more thoroughly later in this International Standard;
2. Unbiased: That is, each potential outcome has the same chance of occurring; and
3. Independent: The coin flip is said to be uncorrelated, memoryless or historyless; whatever happened before the current flip does not influence it.

Such a series of idealized coin flips is directly applicable to a random bit generator. The random bit generators specified in this International Standard will try to simulate a series of idealized coin flips.

5.2 Backward and forward secrecy

As indicated above, unpredictability is a required property of a random bit generator (RBG). It should not be possible to predict the output of a properly implemented and working random bit generator. The inability to predict future output is known as forward secrecy. The inability to determine prior output of an RBG, given knowledge of the current or any future output of the RBG is known as backward secrecy.

Before specifying requirements for forward and backward secrecy, the following factors should be considered.

1. In some instances, achieving backward secrecy is more important than achieving forward secrecy. For example, if a cryptosystem is stolen, an adversary may attempt to read the old messages processed by that system. Forward secrecy is not really a concern, since the system is no longer in use by the original owner. Achieving backward secrecy is straightforward (for example by the appropriate use of a one-way function in the design), although there may be a performance cost associated with providing this property, depending on the design.
2. Trying to achieve forward secrecy may not be appropriate for some cryptosystems. For example, a smart card may be initialised at the point of manufacture with sufficient entropy in the seed and is set to expire after a limited time (e.g., two or three years). In this case, it may be much easier to replace the card with a new smart card that is seeded with a different seed than it is to build forward secrecy into the RBG design.
3. In some instances, achieving forward secrecy may be more important than achieving backward secrecy. Consider, for example, the secure generation of nonces. It is not necessary for a random bit generation algorithm to have backward secrecy as all of the previous outputs will be known. However, forward secrecy may be useful to prevent an adversary with knowledge of the generator from being able to predict later outputs.

The decision whether to incorporate backward and/or forward secrecy is determined by the requirements of the consuming application.

5.3 Top-level objectives and requirements for a random bit generator (RBG) output

The top-level objectives and requirements provided below are fundamental to the security of cryptographic mechanisms that require random input.

The objectives and requirements treat the RBG as a black box, and therefore, apply to any random bit generator, either deterministic or non-deterministic. The requirements are, basically, variations on what it means for the output bit stream to be sufficiently random.

The threshold between feasible and infeasible shall be determined by the overall requirement for the minimum acceptable strength of cryptographic security required by the application.

The top-level objectives and requirements for RBG output streams are as follows.

1. Under reasonable assumptions, it shall not be feasible to distinguish the output of the RBG from true random bits that are uniformly distributed. Informally, all possible outputs occur with equal probability and a series of outputs appears to conform to the uniform distribution.
2. Given a sequence of output bits, it shall not be known to be feasible to compute or predict any other output bit, either past or future.
3. The output stream shall not repeat in the RBG life time except strictly by chance.
4. The RBG output shall not leak secret information, such as the internal state, from the perspective of an adversary.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

5.4 Top-level objectives and requirements for RBG operation

The top-level objectives and requirements for the operation of an RBG are as follows.

1. The RBG shall not generate bits unless the generator has been assessed to possess sufficient entropy. The criteria for sufficiency shall be the greater of the requirements of this International Standard and the requirements of the consuming application.
2. On detection of an error, the RBG shall either (a) enter a permanent error state, or (b) be able to recover from a loss or compromise of entropy if the permanent error state is deemed unacceptable for the application requirements. These requirements may be satisfied procedurally or innately in the design.
3. The design and implementation of an RBG shall have a defined protection boundary, for example, an ISO/IEC 19790 cryptographic module boundary (see Annex I).
4. The RBG output shall not leak secret information (e.g., internal state).
5. The probability that the RBG can “misbehave” in some pathological way that violates the output requirements (e.g., constant output or small cycles, i.e., looping such that the same output is repeated) shall be sufficiently small. That means that the probability of error should be consistent with the overall confidence in correct operation that is required of the RBG, which need not be the same as the required strength of cryptographic security.
6. The RBG design shall include methods to prohibit predictable influence, manipulation, or predicting the output of the RBG by observing the generator's physical characteristics (e.g., power consumption, timing or emissions).

Possible optional features for the operation of an RBG are as follows.

1. If the RBG is capable of operating in more than one mode, the RBG should return information about the mode in which it is operating, upon the request.