INTERNATIONAL STANDARD

ISO/IEC 18031

Second edition
2011-11-15

Information technology — Security techniques — Random bit generation

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

Reference number
ISO/IEC 18031:2011(E)



© ISO/IEC 2011



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2011

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 Properties and requirements of an RBG 6
5.1 Properties of an RBG 6
5.2 Requirements of an RBG 7
5.3 Optional requirements for an RBG 8

6 RBG model 8
6.1 Conceptual functional model for random bit generation 8
6.2 RBG basic components 9
6.2.1 Introduction to the RBG basic components 9
6.2.2 Entropy source 10
6.2.3 Additional inputs 10
6.2.4 Internal state 11
6.2.5 Internal state transition functions 12
6.2.6 Output generation function 13
6.2.7 Support functions 13

7 Types of RBGs 14
7.1 Introduction to the types of RBGs 14
7.2 Non-deterministic random bit generators 14
7.3 Deterministic random bit generators 15
7.4 The RBG spectrum 15

8 Overview and requirements for an NRBG 16
8.1 NRBG overview 16
8.2 Functional model of an NRBG 16
8.3 NRBG entropy sources 18
8.3.1 Primary entropy source for an NRBG 18
8.3.2 Physical entropy sources for an NRBG 20
8.3.3 NRBG non-physical entropy sources 20
8.3.4 NRBG additional entropy sources 21
8.3.5 Hybrid NRBGs 22
8.4 NRBG additional inputs 22
8.4.1 NRBG additional inputs overview 22
8.4.2 Requirements for NRBG additional inputs 22
8.5 NRBG internal state 23
8.5.1 NRBG internal state overview 23
8.5.2 Requirements for the NRBG internal state 23
8.5.3 Optional requirements for the NRBG internal state 24
8.6 NRBG internal state transition functions 24
8.6.1 NRBG internal state transition functions overview 24
8.6.2 Requirements for the NRBG internal state transition functions 25
8.6.3 Optional requirements for the NRBG internal state transition functions 25
8.7 NRBG output generation function 26
8.7.1 NRBG output generation function overview 26
8.7.2 Requirements for the NRBG output generation function 26

© ISO/IEC 2011 – All rights reserved

8.7.3 An optional requirement for the NRBG output generation function 26
8.8 NRBG health tests 26
8.8.1 NRBG health tests overview 26
8.8.2 General NRBG health test requirements 27
8.8.3 NRBG health test on deterministic components 27
8.8.4 NRBG health tests on entropy sources 28
8.8.5 NRBG health tests on random output 29
8.9 NRBG component interaction 31
8.9.1 NRBG component interaction overview 31
8.9.2 Requirements for NRBG component interaction 31
8.9.3 Optional requirements for NRBG component interaction 31

9 Overview and requirements for a DRBG 31
9.1 DRBG overview 31
9.2 Functional model of a DRBG 32
9.3 DRBG entropy source 34
9.3.1 Primary entropy source for a DRBG 34
9.3.2 Generating seed values for a DRBG 36
9.3.3 Additional entropy sources for a DRBG 36
9.3.4 Hybrid DRBG 37
9.4 Additional inputs for a DRBG 37
9.5 Internal state for a DRBG 37
9.6 Internal state transition function for a DRBG 38
9.7 Output generation function for a DRBG 39
9.8 Support functions for a DRBG 39
9.8.1 DRBG support functions overview 39
9.8.2 DRBG health test 39
9.8.3 DRBG deterministic algorithm test 40
9.8.4 DRBG software/firmware integrity test 40
9.8.5 DRBG critical functions test 40
9.8.6 DRBG software/firmware load test 40
9.8.7 DRBG manual key entry test 40
9.8.8 DRBG continuous random bit generator test 40
9.9 Additional requirements for DRBG keys 41

Annex A (normative) **Combining RBGs** 43

Annex B (normative) **Conversion methods** 44
B.1 Random number generation 44
B.1.1 Techniques for generating random numbers 44
B.1.2 The simple discard method 44
B.1.3 The complex discard method 44
B.1.4 The simple modular method 45
B.1.5 The complex modular method 45
B.2 Extracting bits in the Dual_EC_DRBG 46
B.2.1 Potential bias in an elliptic curve over a prime field F_p 46
B.2.2 Adjusting for the missing bit(s) of entropy in the x coordinates 47
B.2.3 Values for E 48
B.2.4 Observations 50

Annex C (normative) **DRBGs** 51
C.1 DRBG mechanism examples 51
C.2 DRBGs based on hash-functions 51
C.2.1 Introduction to DRBGs based on hash-functions 51
C.2.2 Hash_DRBG 51
C.2.3 HMAC_DRBG 59
C.3 DRBGs based on block ciphers 65
C.3.1 Introduction to DRBGs based on block ciphers 65
C.3.2 CTR_DRBG 65
C.3.3 OFB_DRBG 74
C.4 DRBGs based on number theoretic problems 76
C.4.1 Introduction to DRBGs based on number theoretic problems 76

 © ISO/IEC 2011 – All rights reserved

C.4.2 Dual Elliptic Curve DRBG (Dual_EC_DRBG) **76**
C.4.3 Micali Schnorr DRBG (MS_DRBG) **85**
C.5 DRBG based on multivariate quadratic equations **95**
C.5.1 Introduction to a DRBG based on multivariate quadratic equations **95**
C.5.2 Multivariate Quadratic DRBG (MQ_DRBG) **95**

Annex D (normative) **Application specific constants** **107**
D.1 Constants for the Dual_EC_DRBG **107**
D.1.1 Introduction to Dual_EC_DRBG required constants **107**
D.1.2 Curves over prime fields **107**
D.1.3 Curves over binary fields **110**
D.2 Default moduli for the MS_DRBG (…) **120**
D.2.1 Introduction to MS_DRBG default moduli **120**
D.2.2 Default modulus *n* of size 1024 bits **120**
D.2.3 Default modulus *n* of size 2048 bits **120**
D.2.4 Default modulus *n* of size 3072 bits **120**
D.2.5 Default modulus *n* of size 7680 bits **120**
D.2.6 Default modulus *n* of size 15360 bits **121**

Annex E (informative) **NRBG examples** **123**
E.1 Canonical coin tossing example **123**
E.1.1 Overview **123**
E.1.2 Description of basic process **123**
E.1.3 Relation to standard NRBG components **123**
E.1.4 Optional variations **124**
E.1.5 Peres unbiasing procedure **124**
E.2 Hypothetical noisy diode example **125**
E.2.1 Overview **125**
E.2.2 General structure **125**
E.2.3 Details of operation **126**
E.2.4 Failsafe design consequences **130**
E.2.5 Modified example **130**
E.3 Mouse movement example **130**

Annex F (informative) **Security considerations** **132**
F.1 Attack model **132**
F.2 The security of hash-functions **132**
F.3 Algorithm and key size selection **132**
F.3.1 Introduction **132**
F.3.2 Equivalent algorithm strengths **133**
F.3.3 Selection of appropriate DRBGs **134**
F.4 The security of block cipher DRBGs **135**
F.5 Conditioned entropy sources and the derivation function **135**

Annex G (informative) **Discussion on the estimation of entropy** **136**

Annex H (informative) **RBG assurance** **137**

Annex I (informative) **RBG boundaries** **138**

Annex J (informative) **Rationale for the design of statistical tests** **140**
J.1 Introduction **140**
J.2 Runs test **140**
J.3 Long runs test **140**

Bibliography **142**

© ISO/IEC 2011 – All rights reserved

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.

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 joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national 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 and IEC 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*.

This second edition cancels and replaces the first edition (ISO/IEC 18031:2005), which has been technically revised. It also incorporates the Technical Corrigendum ISO/IEC 18031:2005/Cor.1:2009.

© ISO/IEC 2011 – All rights reserved

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.

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.

It is possible to categorize random bit generators into two types. 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, 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.

NOTE This International Standard also recognizes and discusses the existence of Hybrid Random Bit Generators.

© ISO/IEC 2011 – All rights reserved

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

- specifies the characteristics of the main elements required for a non-deterministic random bit generator,
- specifies the characteristics of the main elements required for a deterministic random bit generator,
- establishes the security requirements for both the non-deterministic and the deterministic random bit generator.

Where there is a requirement to produce sequences of random numbers from random bit strings, Annex B gives guidelines 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 9797-2, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 2: Mechanisms using a dedicated hash-function*

ISO/IEC 10116, *Information technology — Security techniques — Modes of operation for an n-bit block cipher*

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

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

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

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

© ISO/IEC 2011 – All rights reserved