INTERNATIONAL STANDARD

ISO/IEC 18031

Second edition
2011-11-15

AMENDMENT 1
2017-02

Information technology — Security techniques — Random bit generation

AMENDMENT 1: Deterministic random bit generation

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

AMENDEMENT 1: Génération déterministe de bits aléatoires

Reference number
ISO/IEC 18031:2011/Amd.1:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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 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 on 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 the following URL: www.iso.org/iso/foreword.html.

Amendment 1 to ISO/IEC 18031-1:2011 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Information technology — Security techniques — Random bit generation

AMENDMENT 1: Deterministic random bit generation

Page 141

Add a new Annex K.

Annex K
(informative)
Example cases for MQ_DRBG

K.1 General

Annex K and its supporting files provides example cases for 14 settings listed in ISO/IEC 18031:2011, Table C.5. The supporting files are available at the following URL:

http://standards.iso.org/iso/18031/

In each of the 14 settings described in Annex K, the bitstring *P* provides a randomly selected system of multivariate quadratic equations that complies with the selection rules of C.5.2.5. The rank distribution resulting from the verification of rank conditions is detailed for each setting.

P is given in the format described in C.5.2.4 which is recalled below. Each example case also includes a sequence of consecutive input-output pairs for the **Evaluate_MQ**(*...*) function.

K.1.1 Format for representing field elements

Each system coefficient is an element of the binary field GF(2^{field_size}) and is a univariate polynomial over GF(2) modulo the irreducible polynomial given in Table C.6. A field element is handled as a bitstring of *field_size* bits composed of its GF(2) coefficients ordered by decreasing degree. For example, the polynomial $x^3 + x + 1$ in GF(2^4) is represented as the bitstring 1011.

K.1.2 Format for representing a single multivariate quadratic equation

The quadratic system used in MQ_DRBG operates on *n = state_length / field_size* variables and contains *n + m* equations where *m = block_length / field_size*. A quadratic equation is written as the concatenation of its coefficients in lexicographic order and by decreasing degree. Therefore the coefficient of the monomial x_1x_1 appears first, followed by that of x_1x_2 and so forth, up to the coefficient of x_1x_n. The coefficient of the monomial x_2x_2 appears next, followed by that of x_2x_3 and so forth, until the last quadratic coefficient $x_{n-1}x_n$ is reached. Then linear coefficients appear, starting with the coefficient of the monomial x_1 and ending with that of x_n. When *field_size* = 1, the linear coefficients are omitted since the underlying field is GF(2) and $x_ix_i = x_i$. The string ends with the constant coefficient of the quadratic equation.

K.1.3 Format for representing a complete system of quadratic equations

The quadratic system encoded into the bitstring *P* contains its *n + m* quadratic equations concatenated in sequential order, starting with the coefficients of the first equation and ending with those of the (*n+m*)-th equation. *P* is formed by the resulting bit string of length *system_length*.

K.1.4 Format for representing inputs and outputs

The input x to **Evaluate_MQ**(P, x) is a vector of n field elements and is given as a bitstring formed by concatenating their bitstring representations, starting with x_1 and ending with x_n. Similarly, the output $y \,||\, z$ is a vector of $n + m$ field elements represented in the same format.

K.1.5 Summary of example cases

Table K.1 summarizes the 14 example cases.

Table K.1 — Summary of example cases

requested_strength	*block_length*			
	112	128	192	256
80	K.2 Binary field GF(2) $n = 112$ $m = 112$ $\mathit{min\_weight} = 4$ $\mathit{min\_rank} \geq 106$	K.4 Binary field GF(2^4) $n = 32$ $m = 32$ $\mathit{min\_weight} = 5$ $\mathit{min\_rank} \geq 30$	K.7 Binary field GF(2^6) $n = 32$ $m = 32$ $\mathit{min\_weight} = 5$ $\mathit{min\_rank} \geq 30$	K.11 Binary field GF(2^8) $n = 32$ $m = 32$ $\mathit{min\_weight} = 5$ $\mathit{min\_rank} \geq 30$
112	K.3 Binary field GF(2) $n = 120$ $m = 112$ $\mathit{min\_weight} = 4$ $\mathit{min\_rank} \geq 114$	K.5 Binary field GF(2) $n = 128$ $m = 128$ $\mathit{min\_weight} = 4$ $\mathit{min\_rank} \geq 122$	K.8 Binary field GF(2^4) $n = 48$ $m = 48$ $\mathit{min\_weight} = 5$ $\mathit{min\_rank} \geq 44$	K.12 Binary field GF(2^4) $n = 64$ $m = 64$ $\mathit{min\_weight} = 5$ $\mathit{min\_rank} \geq 60$
128		K.6 Same as K.5	K.9 Binary field GF(2^3) $n = 64$ $m = 64$ $\mathit{min\_weight} = 5$ $\mathit{min\_rank} \geq 60$	K.13 Same as K.12
192			K.10 Binary field GF(2) $n = 200$ $m = 192$ $\mathit{min\_weight} = 4$ $\mathit{min\_rank} \geq 192$	K.14 Binary field GF(2^2) $n = 128$ $m = 128$ $\mathit{min\_weight} = 5$ $\mathit{min\_rank} \geq 124$
256				K.15 Binary field GF(2) $n = 272$ $m = 256$ $\mathit{min\_weight} = 4$ $\mathit{min\_rank} \geq 264$

K.2 Example case for *requested_strength* = 80 and *block_length* = 112

K.2.1 System of multivariate quadratic equations

The bitstring *P* containing the system coefficients is provided in digital form in the file “coefficients-BL-112-Sec-80-F2.bin” in accordance with the format described in K.1.3.

The file contains 177212 bytes and its SHA-1 checksum in hexadecimal form is

95d78546df132777af932886a887da96aa9afa46

The ranks are distributed as follows:

106: 4561

108: 2213145

110: 58156950

112: 43613144

Sum: 103987800

K.2.2 Inputs and outputs

The bitstrings *x*, *y* and *z* are provided in digital form in accordance with the format described in K.1.4. Their hexadecimal values are:

x = 0000000000000000000000000001

y = bb8cf180cbc3a6002c19c770ed0d

z = 7847b864cfadf70fb359203e06d8

x = bb8cf180cbc3a6002c19c770ed0d

y = a1e0811b5b7733113ca8e22dd2b1

z = 57d27f7b0fc67aec0d5e8115cd93

x = a1e0811b5b7733113ca8e22dd2b1

y = 634ae5294dbc4cc79ce11cfeb1d7

z = c42c5cc5b5b61396df3fcf7a4e2b

x = 634ae5294dbc4cc79ce11cfeb1d7

y = 36701faea23130a0407a44f5e420

z = bf3ddd3cbb141fcd96cbba66ebb9

x = 36701faea23130a0407a44f5e420

y = 74b5baa1095f61eb6b15d317d5ed

z = 7f4ad5787a0c5451bddcf2aef533

x = 74b5baa1095f61eb6b15d317d5ed

y = 62804addbe9da290c38e9de0fe71

z = 5f1f209b62cce21f75d9d03607a9

x = 62804addbe9da290c38e9de0fe71

y = 7d0892da52eed7facc377af1918f

z = 69d5bef53c03fa33a0273cf44c21

x = 7d0892da52eed7facc377af1918f

y = 8ee43a16842345d4cd182852cdea

z = ed479a677e6c2a3cffbbada0e765

x = 8ee43a16842345d4cd182852cdea

y = 2eb8cc9185445b2bab3f4b504aaf

z = 9407f0fe9393fa335051ac2bf414

x = 2eb8cc9185445b2bab3f4b504aaf

y = 8deb10cb70bc3818209a576fb5cb

z = 6106cb8aa8e9a7de949a506b2278

K.3 Example case for *requested_strength* = 112 and *block_length* = 112

K.3.1 System of multivariate quadratic equations

The bitstring P containing the system coefficients is provided in digital form in the file “coefficients-BL-112-Sec-112-F2.bin” in accordance with the format described in K.1.3.

The file contains 210569 bytes and its SHA-1 checksum in hexadecimal form is

ae1c4ea33afc96e3aa421f6456055a7c7ee33989

The ranks are distributed as follows:

114: 5239

116: 2551294

118: 66936700

120: 50200265

Sum: 119693498

K.3.2 Inputs and outputs

The bitstrings *x*, *y* and *z* are provided in digital form in accordance with the format described in K.1.4. Their hexadecimal values are:

x = 000000000000000000000000000001

y = 46609cda28057a917a08b60a1d969d

z = a06fe3e456a8c24315dfde6088bd

x = 46609cda28057a917a08b60a1d969d

y = 37d12de7b69f2170ba8717e96f0f43

z = 8fb9899c9e2d4ef33056aadf946d

x = 37d12de7b69f2170ba8717e96f0f43

y = 463860297cec60797650c4897563d4

z = 89745528548d7bd3a2c9e5afd3fc

x = 463860297cec60797650c4897563d4

y = 6a4c5b16c156738e9b07c4c2c2818e

z = 5f9f14194e601f48657164f34e34

x = 6a4c5b16c156738e9b07c4c2c2818e

y = 289c50a28bb48a685703eb425597dd

z = c9dae7a3c32a01648a32d91b8728

x = 289c50a28bb48a685703eb425597dd

y = 4d96224af4aeaac54d8472374f645d

z = cf7a6cc73793049241497ee26603

x = 4d96224af4aeaac54d8472374f645d

y = df5ac81223125d967056d5dcdba088

z = 3d9741ec702076fe8473b7181aa9

x = df5ac81223125d967056d5dcdba088

y = 41a1df8cc57c402f520d671464b728

z = 285d6b741e417e417b9f8fa87356

x = 41a1df8cc57c402f520d671464b728

y = 0af3539a48bc07e3afb00d3c529ff5

z = e6d4d36dcc2cca4826b94e76be10

x = 0af3539a48bc07e3afb00d3c529ff5

y = e2f7d8f01d2ae145a643b9351ada76

z = 29bdd54840cf84027f20e48ce195

K.4 Example case for *requested_strength* = 80 and *block_length* = 128

K.4.1 System of multivariate quadratic equations

The bitstring *P* containing the system coefficients is provided in digital form in the file “coefficients-BL-128-Sec-80-F16.bin” in accordance with the format described in K.1.3.

The file contains 17952 bytes and its SHA-1 checksum in hexadecimal form is

d6614e19bd953ca88ff49f016b80f5ac17b7dab1

The ranks are distributed as follows:

30: 520948

32: 7782684

Sum: 8303632

K.4.2 Inputs and outputs

The bitstrings *x, y* and *z* are provided in digital form in accordance with the format described in K.1.4. Their hexadecimal values are:

x = 00000000000000000000000000000001

y = f719e81ed992ca7c793258b5251d0534

z = 66092272f74a85ecaef639d78ed9831f

x = f719e81ed992ca7c793258b5251d0534

y = 37614b89b9bbd6eea4560ecb3bdb8807

z = 96b4c1aeb27aa47fbc7a3b1464343736

x = 37614b89b9bbd6eea4560ecb3bdb8807

y = 136bf7d8fbcbabd37a2baa321a5d94f7

z = 29141359d8099496eaf84ae3d863591a

x = 136bf7d8fbcbabd37a2baa321a5d94f7

y = bc6316205ac244b4fc8dcee70f423874

z = d8005ccefa012118820cf02c9eb4328d

x = bc6316205ac244b4fc8dcee70f423874

y = 64d8adbf03a6418fa549f235e5f84bcd

z = 9c0aad312ef00336d0f055e81f2b3677

x = 64d8adbf03a6418fa549f235e5f84bcd

y = 3ac1c733b68ca734550343d950649d5a

z = 1f07210c4a6d4fd784ee0f9f9789c5ab

x = 3ac1c733b68ca734550343d950649d5a

y = 1a22cbbe771e641373700306718dbf6e

z = ba8064102a7e8d714e92e0dfddfbe607

x = 1a22cbbe771e641373700306718dbf6e

y = fa2eabf2c9794f6b9bac6561409aab0d

z = 7e2bae34daaf284557bbe5ae48e54d26

x = fa2eabf2c9794f6b9bac6561409aab0d

y = 46f6f74d23504a64565b2c35cd0036df

z = c6285e77cbf16150457d03bfc6015ef7

x = 46f6f74d23504a64565b2c35cd0036df

y = 729bc30c32fd7fec1ccb95bc4aabfa27

z = 963bda8ab7dc84ee2dd5a60a9c4392cd

K.5 Example case for *requested_strength* = 112 and *block_length* = 128