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) $n = 112$ $m = 112$ *min_weight* = 4 *min_rank* ≥ 106	K.4 Binary field GF(2^4) $n = 32$ $m = 32$ *min_weight* = 5 *min_rank* ≥ 30	K.7 Binary field GF(2^6) $n = 32$ $m = 32$ *min_weight* = 5 *min_rank* ≥ 30	K.11 Binary field GF(2^8) $n = 32$ $m = 32$ *min_weight* = 5 *min_rank* ≥ 30
112	K.3 Binary field GF(2) $n = 120$ $m = 112$ *min_weight* = 4 *min_rank* ≥ 114	K.5 Binary field GF(2) $n = 128$ $m = 128$ *min_weight* = 4 *min_rank* ≥ 122	K.8 Binary field GF(2^4) $n = 48$ $m = 48$ *min_weight* = 5 *min_rank* ≥ 44	K.12 Binary field GF(2^4) $n = 64$ $m = 64$ *min_weight* = 5 *min_rank* ≥ 60
128		K.6 Same as K.5	K.9 Binary field GF(2^3) $n = 64$ $m = 64$ *min_weight* = 5 *min_rank* ≥ 60	K.13 Same as K.12
192			K.10 Binary field GF(2) $n = 200$ $m = 192$ *min_weight* = 4 *min_rank* ≥ 192	K.14 Binary field GF(2^2) $n = 128$ $m = 128$ *min_weight* = 5 *min_rank* ≥ 124
256				K.15 Binary field GF(2) $n = 272$ $m = 256$ *min_weight* = 4 *min_rank* ≥ 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 = 00000000000000000000000000001

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 = 00000000000000000000000000000001

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

K.5.1 System of multivariate quadratic equations

The bitstring *P* containing the system coefficients is provided in digital form in the file "coefficients-BL-128-Sec-112-F2.bin" in accordance with the format described in K.1.3.

The file contains 264224 bytes and its SHA-1 checksum in hexadecimal form is

fcd983e78ddd489a9425be58b8139e04c89fb6c6

The ranks are distributed as follows:

122: 7704

124: 3783524

126: 99303857

128: 74493971

Sum: 177589056

K.5.2 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 = c04f664eb59219b1e6b0d0e0fc5ae660

z = 894f5e21cc208ce73ebb136c0c7b6e47

x = c04f664eb59219b1e6b0d0e0fc5ae660

y = 10da311bd87ba42fd89a17f45b0b0931

z = f3561e3a42a23037d04b7991e44f98d0

x = 10da311bd87ba42fd89a17f45b0b0931

y = c42c14916632d8518f435796c069a381

z = 461593a9b73573772cf8f8a93020eada

x = c42c14916632d8518f435796c069a381

y = 325ebb605c4037b6092a7952adedd16d

z = 3f80f69b2f81f012994189125cba6b00

x = 325ebb605c4037b6092a7952adedd16d

y = 596cdd4392413988fa7a15fa7fb5d74b

z = 8ec0f223da49f826f6faf8d25b54b231

x = 596cdd4392413988fa7a15fa7fb5d74b

y = 17790ac47b8112312631c0e3b0066fd0

z = 8d98258ade35f74057a98542c0d7d937

x = 17790ac47b8112312631c0e3b0066fd0

y = d76a00f9e3318091e0f113b48f0cb752

z = 8b9664e30122848541b91743171b4812

x = d76a00f9e3318091e0f113b48f0cb752

y = 4ffffdf6def93bb391d90312a801ece5

z = d17acb75d2f57976df164061716601e0

x = 4ffffdf6def93bb391d90312a801ece5

y = 89b596d08123105f5994679f5e428136

z = 1de72c77e98fa45090197c81e4d2a3a3

x = 89b596d08123105f5994679f5e428136

y = 7294da76d6d2bf9dfb9d2c1d03ca4928

z = 96cea7ffad3bc8be151106cd4c067565

K.6 Example case for *requested_strength* = 128 and *block_length* = 128

The example case is the same as in K.5.

K.7 Example case for *requested_strength* = 80 and *block_length* = 192

K.7.1 System of multivariate quadratic equations

The bitstring P containing the system coefficients is provided in digital form in the file "coefficients-BL-192-Sec-80-F64.bin" in accordance with the format described in K.1.3.

The file contains 26928 bytes and its SHA-1 checksum in hexadecimal form is

dad206d21189e0b9aaa5bb60298e0cf3f918ae81

The ranks are distributed as follows:

30: 129895

32: 8173737

Sum: 8303632

K.7.2 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 = 000000000000000000000000000000000000000000000001

y = 9b021d45d52d7637ca3350732d880265bc826a1a7e9969b4

z = f5df581e7eb83f86d7f1101b248b4740662733897f4b4689

x = 9b021d45d52d7637ca3350732d880265bc826a1a7e9969b4

y = 937625307ba580d0763a6272e3ba7d9256536795a0017b7c

z = 338d582a1b8c37812aed0f07f2958101f11ac11ee962a02a

x = 937625307ba580d0763a6272e3ba7d9256536795a0017b7c

y = d9d32553f1299fcd1444030c23f084d1c85fd08a2ef5275b

z = 9bb8f5de5ff6c6aba79ae510429221a6dc3b0ab7ef1b27ca

x = d9d32553f1299fcd1444030c23f084d1c85fd08a2ef5275b

y = 329800d2a8f045893d24c54d6993e67e0e2c34b2956ee269

z = 0a01d2046afc3adbd68e024f1205ca00cee736e53c7aaabe

x = 329800d2a8f045893d24c54d6993e67e0e2c34b2956ee269

y = 723a5476da2e4617f9418545014266ac7179f591451952e9

z = 5cf9cfeefb0d0eb2985a4cc8e66c7ba0fcf332971a4ebad

x = 723a5476da2e4617f9418545014266ac7179f591451952e9

y = 67786dd966efde83df99af5f6059f4c3f07f84fe5ae1d656

z = f68fa0ae09b71a71f780550280204bb9430318733649ea3d

x = 67786dd966efde83df99af5f6059f4c3f07f84fe5ae1d656

y = 03ecc9b12c99215531b56f5a99e5407d5c343ac6b7793c54

z = 34a9a04510415ad411fc14f8046f6538e4df891b1744462d

x = 03ecc9b12c99215531b56f5a99e5407d5c343ac6b7793c54

y = 8bf2fd718e72802e62209a681399d08f609142e3745c5af0

z = 18f2e2af78854c66b7aaffc9ece76c981e4080ebb1bafa89

x = 8bf2fd718e72802e62209a681399d08f609142e3745c5af0

y = e2424fdcdfd6bc8e02ff7a4bc445190945e7292af2aa8926

z = e2f2ee9d272702f367f73456604eb633c01bdeadacc2d6ef

x = e2424fdcdfd6bc8e02ff7a4bc445190945e7292af2aa8926

y = d94f6dc6299ae4069f06333edb94335e4553b4e20cfe9896

z = 1acb06c4e696cc73520197e331aad76185d6d246f2115d32

K.8 Example case for *requested_strength* = 112 and *block_length* = 192

K.8.1 System of multivariate quadratic equations

The bitstring P containing the system coefficients is provided in digital form in the file "coefficients-BL-192-Sec-112-F16.bin" in accordance with the format described in K.1.3.

The file contains 58800 bytes and its SHA-1 checksum in hexadecimal form is

151f9a4c9b32f6e9236ae071408bbba39b597585

The ranks are distributed as follows:

44: 2

46: 4054618

48: 60538940

Sum: 64593560

K.8.2 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 = 000000000000000000000000000000000000000000000001

y = 4bc49157a1cfc4e81a00e38073c3c330716846f262fd6bd8

z = 9f9c37ccbf0351e173402c9778721e07b7f92e7ad9c13a0c

x = 4bc49157a1cfc4e81a00e38073c3c330716846f262fd6bd8

y = efd8d72753ca6319ad85e8632a2731082e24851cb496517b

z = 3b6ed30bfac7560230730efa2befd0b63c610ddc84579b47

x = efd8d72753ca6319ad85e8632a2731082e24851cb496517b
y = 6817118a48c2faae74cd95654416f072c44dfd2309bb216d
z = e2dd5934948ac3f16f4dcd5e1343104e8a69fc004e700ae1

x = 6817118a48c2faae74cd95654416f072c44dfd2309bb216d
y = 668a844f1fd85b03eb5ace651179ba6adb6080dda180dfc0
z = 78f8d2f16f0c1cdb96b7eeef95e8d852267d2599bfd0a3a5

x = 668a844f1fd85b03eb5ace651179ba6adb6080dda180dfc0
y = 84f988e9a1335ceaa21e526bd1df380d137a7470ad2167fb
z = d459b9f5ac1ab0622e324994bd1c70038e1e500d6ed21c87

x = 84f988e9a1335ceaa21e526bd1df380d137a7470ad2167fb
y = 5f3263e90c40060d975443ca13dc9388f01bec3c3f3d28ea
z = b427e405b17d64c91a9e8622a896d20c7c75a8ad5139ccbf

x = 5f3263e90c40060d975443ca13dc9388f01bec3c3f3d28ea
y = 7f4a9db932fff536a7f5df253d8e974ae6852866d2558629
z = b23c1c8f7fff065e9b9827b65b6f3d156d4c8bc1343b173c

x = 7f4a9db932fff536a7f5df253d8e974ae6852866d2558629
y = 5e1395441cb914d8ad706f7c9c03ccc73e5780c2e44f5504
z = 284e181d513eb5e9bebde7d78f6c8ed52bec0ffda2a96634

x = 5e1395441cb914d8ad706f7c9c03ccc73e5780c2e44f5504
y = 9a28d4de9d2a5dae64c38a936c672072e90f60f71fa1cbf9
z = e41bb6b73ba2052d035d07f8dc5cb40d15f1eca51fbd6e0e

x = 9a28d4de9d2a5dae64c38a936c672072e90f60f71fa1cbf9
y = 66660d18cf3651da98e89f566bf00355cca6c0baf9a2d1c1
z = 601c8b113003889e0348566729e8e0751f53c294f5dbe000

K.9 Example case for *requested_strength* = 128 and *block_length* = 192

K.9.1 System of multivariate quadratic equations

The bitstring *P* containing the system coefficients is provided in digital form in the file "coefficients-BL-192-Sec-128-F8.bin" in accordance with the format described in K.1.3.

The file contains 102960 bytes and its SHA-1 checksum in hexadecimal form is

b286f9cad81b0b718ead54180239eba7d3b4d14a

The ranks are distributed as follows:

60: 1089

62: 34926475

64: 240656468

Sum: 275584032

K.9.2 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 = 00000000000000000000000000000000000000000000000000000001

y = 762258ce8826f6d2dd46a7c6784733f050929aa23ab60ee8

z = 1155bc183f9c8fa8ed268a4bae7256b7f2c456f3729b5d0b

x = 762258ce8826f6d2dd46a7c6784733f050929aa23ab60ee8

y = 02e827998b27a602323923e9db9c48750316d0e055556622

z = 3127eeb8f998fd23ed59e9993263ee5cd6cec2a221bb6ce5

x = 02e827998b27a602323923e9db9c48750316d0e055556622

y = bd469c2e97afbc180f8b023205e46c060a6bc453ef5898d3

z = c1586f6694edfbc5cf7b269136fdddcb392129e938453cf2

x = bd469c2e97afbc180f8b023205e46c060a6bc453ef5898d3

y = 293f502e6b12185832844d5850f7a08ce4229e567adeea11

z = 7541eb4affc5517ead8430e2701c94d50b461e14e063543d

x = 293f502e6b12185832844d5850f7a08ce4229e567adeea11

y = 15f0f194a952f1c98eb5d4449a3b21d8dfa0b068982b19df

z = 71f515a88870778b7194870180fb7bd963960c44d43fc4f0

x = 15f0f194a952f1c98eb5d4449a3b21d8dfa0b068982b19df

y = bce241c8b0ea940679bad3c259860ff978d7efaad313aed7

z = 0a37faed572b12a1a0fb5167a69bab22d1093a051cbeb725

x = bce241c8b0ea940679bad3c259860ff978d7efaad313aed7

y = fe7bf955dbd9b517d516ce81584985f54bc93229bd0baf97

z = b29254189ef82d3cb673c2c17ded8378a3effbc323e09095

x = fe7bf955dbd9b517d516ce81584985f54bc93229bd0baf97

y = 3b0ab7a9534dc16df8dbc8f921049bf24163009c7a468684

z = c7d85ea5c1adc569c435db47135c20c63ae525b18fe6d5b0

x = 3b0ab7a9534dc16df8dbc8f921049bf24163009c7a468684

y = 421b005096b17b479d04215fdd7262e86460fe7c0e439949

z = bf3f9480e4f1fb02ad22f94e24063349d68600394a9c2ed4

x = 421b005096b17b479d04215fdd7262e86460fe7c0e439949

y = 9cfd31b93ea12da49b9c176710f7830b43803b20fab8bd51

z = 55a2eee9251283d70798708e1d65e7c23a2f4f06d5841d75

K.10 Example case for *requested_strength* = 192 and *block_length* = 192

K.10.1 System of multivariate quadratic equations

The bitstring P containing the system coefficients is provided in digital form in the file “coefficients-BL-192-Sec-192-F2.bin” in accordance with the format described in K.1.3.

The file contains 984949 bytes and its SHA-1 checksum in hexadecimal form is

3d71baf6bdf23781f11540b36f9f393746902a08

The ranks are distributed as follows:

192: 4

194: 42773

196: 20853635

198: 547456333

200: 410557593

Sum: 978910338

K.10.2 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 = 0000000000000000000000000000000000000000000000000000000000000001

y = ca6ed87127464695c014665de58f55d8c81bbba26d7dbb34f3

z = bee4dcf9847b33da091bb3a50f6b1a1ff8689bc249426711

x = ca6ed87127464695c014665de58f55d8c81bbba26d7dbb34f3

y = 7cc8ea31334cbda06d7bcf77b54a2b4ef5d27771720c2028e7

z = c80918a5a5d501bafc6df7ca2da3891911a899202c5f6da0

x = 7cc8ea31334cbda06d7bcf77b54a2b4ef5d27771720c2028e7

y = 80fb06345c0079dcc5c5c4f875f7174585e5ff0d63b65b1424

z = 7fd6439d40e5bf3f4590bdc7d4887c0d2988f46e1f0cb58e

x = 80fb06345c0079dcc5c5c4f875f7174585e5ff0d63b65b1424

y = ac2e60f576985e0bc4555e5c1a3b78b3bfe98f6f97aac6967e

z = 1a536213fbcd3d18d07c5bc5177daa29f7389508c2fa0d22

x = ac2e60f576985e0bc4555e5c1a3b78b3bfe98f6f97aac6967e

y = 3eb7d7381b1f10098867525a5ab25513a25b74ef5756212963

z = 1001ccf1d6f3ce825973efb492326804f676790d0d3650f8

x = 3eb7d7381b1f10098867525a5ab25513a25b74ef5756212963

y = b9f5fc0d53a53333e0c3f3eecfcd898ebc4d3228fd1f03420a

z = fff44f677a5585fe668f0275a62ab2cc2b221628ccbe4532

x = b9f5fc0d53a53333e0c3f3eecfcd898ebc4d3228fd1f03420a

y = 9b51e0e702e4b72cfab3f8c19b0a39cc577eb3d24603868913

z = b2a6ea5edce91844f3b479d12521e1f362dcc89addc393c8

x = 9b51e0e702e4b72cfab3f8c19b0a39cc577eb3d24603868913

y = 8117c767d4ea992546e091d42ff05ade6f6da391727af34042

z = 3cb7d9104dd79deecfa0cee874385e726bc5c43154c620b2

x = 8117c767d4ea992546e091d42ff05ade6f6da391727af34042

y = 7e8740424081b4f02360920a1f9123c68ae49246e0aed231e1

z = c138871d42aec2ba6e7bfa619d7999e105e7379d5779de79

x = 7e8740424081b4f02360920a1f9123c68ae49246e0aed231e1

y = 43152f18f70c2993caf5dc64ff26be9e8f823e9cf13a5b44f8

z = 20fcbff61224ccc6deccef04f8409842e6670c63ff50fb25

K.11 Example case for *requested_strength* = 80 and *block_length* = 256

K.11.1 System of multivariate quadratic equations

The bitstring P containing the system coefficients is provided in digital form in the file "coefficients-BL-256-Sec-80-F256.bin" in accordance with the format described in K.1.3.

The file contains 35904 bytes and its SHA-1 checksum in hexadecimal form is

25ac05d47b2d1dc9ca21f330b5db4228c06c0552

The ranks are distributed as follows:

30: 32305

32: 8271327

Sum: 8303632

K.11.2 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 = 00000000000000000000000000000000000000000000000000000000000000000000000000000001

y = 845ff78e453e980385e2265728bbbc90c792bafa77bd1d942ac2fcfb4c508963

z = bc5c9f41eb6ce6d3f9936c5cb7cac610f55902149afcdace189b610d254c2bff

x = 845ff78e453e980385e2265728bbbc90c792bafa77bd1d942ac2fcfb4c508963

y = 99dc7f54302df0c04b075e7db6c3c10fbe70a18edf9852b7896f31aa18788192

z = 92f38812133684f0c24cd8a1852df8edd0eaa91828011f3e1b5e2bf5def130d9

x = 99dc7f54302df0c04b075e7db6c3c10fbe70a18edf9852b7896f31aa18788192
y = bf6202d53d315b60b8263a77faf610926d5f479e33bcd899713ae123bb0f5769
z = 7f1d0a9e2895c40c03fe7153e4afc4738ea041593e11adc0eed00749cfc22b04

x = bf6202d53d315b60b8263a77faf610926d5f479e33bcd899713ae123bb0f5769
y = 0ce571d57cc82cb8ab65ad61a2d98af5fd32b0a6315e1cb68c43a6da4b5569f0
z = 9b89a9dba6ae9e51fd4d31fe1a2d0b6396aadae62f1125d9f050f38ef445c704

x = 0ce571d57cc82cb8ab65ad61a2d98af5fd32b0a6315e1cb68c43a6da4b5569f0
y = 3b1210b59b739b1dd0b376ff8db7cc8623892f285f6d3e3608c34a5718318ea1
z = e6f5e3fc89ae09a9658d8518d42f163102f87dc57e779d46b442e11516345ec2

x = 3b1210b59b739b1dd0b376ff8db7cc8623892f285f6d3e3608c34a5718318ea1
y = 2fd0bc4dfdb228a972df094d412cb8369ea68a8ce3c81d7a431bc1264842895e
z = 2e424cdf55c87e859648db33578b025c2ede28e4c822382cd2784e8320f49436

x = 2fd0bc4dfdb228a972df094d412cb8369ea68a8ce3c81d7a431bc1264842895e
y = f73335a5e4fdc5ebe31adf389c1346a7968361b745ad5b69f781bae0eefc54b0
z = 74d2d21284d3deaca76009f5633c33cbd6808cd3bf239b5aab8969034db1ed1f

x = f73335a5e4fdc5ebe31adf389c1346a7968361b745ad5b69f781bae0eefc54b0
y = d64a1e12e8574169dfba54b856415289fafbfae8e7f605af72a15c89b4cf203f
z = 38639991897b5c3f7a0d8adba26abf061e6c4c5532e0514c5029c6c6a20a399d

x = d64a1e12e8574169dfba54b856415289fafbfae8e7f605af72a15c89b4cf203f
y = 011fd95e7497a73cc21e2fd30a6f14a2b3e37e9716e238893e3a81e8a0ff7334
z = 7541b2e6d273efc5d2481b2d9154e92b6c90e73b0fca4e090576a91574c4e9fe

x = 011fd95e7497a73cc21e2fd30a6f14a2b3e37e9716e238893e3a81e8a0ff7334
y = 141bb711f4996dff29382dbb1083e5c30d60d022f65603eb42907a467c934c42
z = 55b876a9a19dad4caeb1c5c4c04efb6e93da1f065c3dee4771d2de484c3180bc

K.12 Example case for *requested_strength* = 112 and *block_length* = 256

K.12.1 System of multivariate quadratic equations

The bitstring *P* containing the system coefficients is provided in digital form in the file "coefficients-BL-256-Sec-112-F16.bin" in accordance with the format described in K.1.3.

The file contains 137280 bytes and its SHA-1 checksum in hexadecimal form is

e975ba3b3ab3b87311a1ab5f62aed2587c20e7de

The ranks are distributed as follows:

60: 23

62: 17286027

64: 258297982

Sum: 275584032

K.12.2 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 = 00000000000000000000000000000000000000000000000000000000000000000000000000000001

y = 0c44dd5a830cb42a0d78978a66e73343712523adf59e2161b7290d45e211208f

z = bb29008dddfd182c7ad58ed9c986046fde8694cbacb45bc2acf201fc1f37916f

x = 0c44dd5a830cb42a0d78978a66e73343712523adf59e2161b7290d45e211208f

y = f12417b73a69d210afef9ded8488b2790c437eafa19c6e7276bb341b0fe8bcf4

z = d895edf6a3f3889b8f8e2b283b2724b7cc428ee78bfce9ef88b041c1e83c1aa0

x = f12417b73a69d210afef9ded8488b2790c437eafa19c6e7276bb341b0fe8bcf4

y = 57c56dcb6db4dcaef4c09859e4a64939781ce90ea94b168987d4b47cb24ddb5c

z = 0f734bb269d9678ae4ec77162e0b175da2d4daf7a8f2211920ca1d1804cfe91f

x = 57c56dcb6db4dcaef4c09859e4a64939781ce90ea94b168987d4b47cb24ddb5c

y = d570b0477acf679409ec942280313d6f479fb1060016d11b942d2f4651f024be

z = 65eeadbc13e38fabb5045c62ea917404996bab6fdf6f4abf930c2f4a8d221d42

x = d570b0477acf679409ec942280313d6f479fb1060016d11b942d2f4651f024be