INTERNATIONAL STANDARD

ISO/IEC 18033-7

First edition
2022-04

Information security — Encryption algorithms —

Part 7: Tweakable block ciphers

Sécurité de l'information — Algorithmes de chiffrement —

Partie 7: Chiffrements par blocs paramétrables

Reference number
ISO/IEC 18033-7:2022(E)

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 or www.iec.ch/members_experts/refdocs).

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 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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 18033 series can be found on the ISO and IEC websites.

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 and www.iec.ch/national-committees.

Introduction

This document specifies tweakable block ciphers. A tweakable block cipher is a family of permutations parametrized by a secret key value and a public tweak value.

Information security — Encryption algorithms —

Part 7: Tweakable block ciphers

1 Scope

This document specifies tweakable block ciphers. A tweakable block cipher is a family of n-bit permutations parametrized by a secret key value and a public tweak value. Such primitives are generic tools that can be used as building blocks to construct cryptographic schemes such as encryption, Message Authentication Codes, authenticated encryption, etc.

A total of five different tweakable block ciphers are defined. They are categorized in Table 1.

Table 1 — Tweakable block ciphers specified

Block length	Tweakey length	Algorithm name
128 bits	256 bits	Deoxys-TBC-256
128 bits	384 bits	Deoxys-TBC-384
64 bits	192 bits	Skinny-64/192
128 bits	256 bits	Skinny-128/256
128 bits	384 bits	Skinny-128/384

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
block
string of bits of a defined length

[SOURCE: ISO/IEC 18033-1:2021 3.5]

3.2
ciphertext
data which has been transformed to hide its information content

[SOURCE: ISO/IEC 18033-1:2021, 3.7]

3.3
encryption algorithm
process which transforms plaintext into ciphertext

[SOURCE: ISO/IEC 18033-1:2021, 3.12]

3.4
key
sequence of symbols that controls the operation of a cryptographic transformation (e.g. encryption, decryption)

[SOURCE: ISO/IEC 11770-1:2010, 2.12, modified – the list of cryptographic mechanisms is removed]

3.5
plaintext
unencrypted information

[SOURCE: ISO/IEC 18033-1:2021, 3.20]

3.6
tweak
non-secret sequence of symbols that controls the operation of a cryptographic transformation (e.g. encryption, decryption)

3.7
tweakable block cipher
symmetric encryption system with the property that the encryption algorithm operates on a block of plaintext, i.e. a string of bits of a defined length, and a *tweakey* (3.8) to yield a block of ciphertext

3.8
tweakey
sequence of symbols that controls the operation of a cryptographic transformation (e.g. encryption, decryption)

Note 1 to entry: The tweakey is the concatenation of the key and the tweak inputs.

4 Symbols

k	key bit-length for a tweakable block cipher
Nr	the number of rounds of the tweakable block cipher
n	plaintext/ciphertext bit-length for a tweakable block cipher
t	tweak bit-length for a tweakable block cipher
$a \leftarrow b$	replaces the value of the variable a with the value of the variable b
$\|\|$	concatenation of bit-strings
$\oplus$	bitwise exclusive-OR operation
M	diffusion matrix of the tweakable block cipher
X	n-bit internal state of the tweakable block cipher
GF(i)	finite field of i elements
$\mathbb{K}$	base field as GF(2^8), defined by the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$

λ sub-tweakey value

ρ table of rotation values for the ShiftRows / ShiftRowsInv functions of Deoxys-TBC and for the ShiftRowsRight / ShiftRowsRightInv of Skinny

h byte permutation in the tweakey schedule algorithm of Deoxys-TBC

P_T cell permutation in the tweakey schedule algorithm of Skinny

$[i, \dots, j]$ sequence of integers starting from i included, ending at j included, with a step of 1

5 Requirements on the usage of tweakable block ciphers

Both Deoxys-TBC and Skinny ciphers propose a tweakey input that can be utilized as key and/or tweak material, up to the user needs. Therefore, the user can freely choose which part of the tweakey is dedicated to key and/or tweak material. However, whatever the combination of key/tweak size chosen by the user, it shall be such that the key size is at least 128 bits.

In general, the tweak may be made public and a user can repeat the same (tweak,key) combination without causing a security degradation. Some use-cases may require stricter conditions to meet the user's security requirements, and these additional conditions shall always be satisfied.

NOTE Modes of operation offering beyond-birthday security are an example for requiring stricter conditions as they often fail if the same tweak is repeated under the same key.

Skinny-64/192 version shall only be used to instantiate security algorithms guaranteeing an upper bound on the adversarial advantage that remains meaningful as long as the adversary processes less than 2^{64} data blocks.

This document describes the Skinny and Deoxys-TBC configuration where the least-significant portion of the tweakey input is loaded with the tweak and the most-significant portion of the tweakey input is loaded with the key material, i.e. tweakey = key || tweak. Keying material shall never be reused across instances with differing tweak sizes.

Annex A provides numerical examples of Deoxys-TBC-256, Deoxys-TBC-384, Skinny-64/192, Skinny-128/256 and Skinny-128/384. Annex B defines the object identifiers which shall be used to identify the algorithms specified in this document.

6 Deoxys-TBC

6.1 Deoxys-TBC versions

The Deoxys-TBC algorithm (originally published in Reference [4], slightly modified for improved performances in Reference [5], the latter being the version described in this document) is a tweakable block cipher. Deoxys-TBC operates on a plaintext block of 16 bytes numbered from most-significant to least-significant byte [0,…,15]. The internal state X of the cipher is a (4×4) matrix of bytes, initialized from the plaintext block of 16 bytes as follows:

$$X = \begin{bmatrix} 0 & 4 & 8 & 12 \\ 1 & 5 & 9 & 13 \\ 2 & 6 & 10 & 14 \\ 3 & 7 & 11 & 15 \end{bmatrix}.$$

This document defines two versions of Deoxys-TBC. For Deoxys-TBC-256 the tweakey is of size 256 bits and consists of a key of size $k \geq 128$ and a tweak of size $t = 256\text{-}k$. For Deoxys-TBC-384 the tweakey is of size 384 bits and consists of a key of size $k \geq 128$ and a tweak of size $t = 384\text{-}k$.

6.2 Deoxys-TBC encryption

The number of rounds *Nr* is 14 for Deoxys-TBC-256 and 16 for Deoxys-TBC-384. One round of Deoxys-TBC encryption, similar to a round in the Advanced Encryption Standard (AES)[3], has the following four transformations applied to the internal state in the order specified below:

— **AddSubTweakey(X, λ)**: bitwise exclusive-or (XOR) the 128-bit round sub-tweakey λ (see 6.4) to the internal state X. This function is applied one more time at the end of the last round.

— **SubBytes(X)**: apply the 8-bit AES Sbox S to each of the 16 bytes of the internal state X. The description of this Sbox in hexadecimal notation is presented in Table 2.

Table 2 — The AES Sbox

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

For example, for an input value `53`, then the output value would be determined by the intersection of the row with index '`5`' and the column with index '`3`', which would give `ed`.

— **ShiftRows(X):** rotate the 4-byte i-th row of the internal state X to the left by $\rho[i]$ positions, where $\rho = (0, 1, 2, 3)$.

— **MixBytes(X):** multiply each column of the internal state X by the (4×4) AES maximum distance separable (MDS) matrix M (given below, coefficients are displayed in their hexadecimal equivalent of the binary representation of bit polynomials from GF(2)[x]) in $\mathbb{K}$, where $\mathbb{K}$ denotes the base field as GF(2^8) defined by the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$.

$$M = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

The composition MixBytes(ShiftRows(SubBytes(X))) is an unkeyed AES round operating on a state X and is denoted AES_R. The encryption with Deoxys-TBC of a 128-bit plaintext P outputs a 128-bit ciphertext C. Denoting the initial internal state by X_0 and the internal state after round i as X_i, a pseudo-code of the algorithm is as follows:

$X_0 \leftarrow P$

$X_{i+1} \leftarrow \text{AES\_R}(\text{AddSubTweakey}(X_i, \lambda_i))$ for i in $[0, \ldots, Nr\text{-}1]$

$C \leftarrow \text{AddSubTweakey}(X_{Nr}, \lambda_{Nr})$

6.3 Deoxys-TBC decryption

For the decryption, at each round the following four transformations are applied to the internal state in the following order:

— **AddSubTweakey(X, λ):** XOR the 128-bit round sub-tweakey λ (See 6.4) to the internal state X. This function is applied one more time at the end of the last round.

— **MixBytesInv(X):** multiply each column of the internal state X by the (4×4) AES MDS matrix M^{-1} (given below, coefficients are displayed in their hexadecimal equivalent of the binary representation of bit polynomials from GF(2)[x]) in $\mathbb{K}$, where $\mathbb{K}$ denotes the base field as GF(2^8) defined by the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$.

$$M^{-1} = \begin{bmatrix} 14 & 11 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 13 & 9 & 14 \end{bmatrix}.$$

— **ShiftRowsInv(X)**: rotate the 4-byte i-th row of the internal state X to the right by $\rho[i]$ positions, where ρ = (0, 1, 2, 3).

— **SubBytesInv(X)**: apply the 8-bit inverse AES Sbox S_inv to each of the 16 bytes of the internal state X. The description of this Sbox in hexadecimal notation is presented in Table 3.

Table 3 — The AES inverse Sbox

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

For example, for an input value `ed`, then the output value would be determined by the intersection of the row with index '`e`' and the column with index '`d`', which would give `53`.

The composition SubBytesInv(ShiftRowsInv(MixBytesInv(X))) is an unkeyed AES inverse round operating on a state X and is denoted AES_R_Inv. The decryption with Deoxys-TBC of a 128-bit ciphertext C outputs a 128-bit plaintext P. Denoting the initial internal state by X_0 and the internal state after round i as X_i, a pseudo-code of the algorithm is as follows: