INTERNATIONAL STANDARD

ISO/IEC 18033-3

Second edition
2010-12-15

Information technology — Security techniques — Encryption algorithms —

Part 3:
Block ciphers

Technologies de l'information — Techniques de sécurité — Algorithmes de chiffrement

Partie 3: Chiffrement par blocs

Reference number
ISO/IEC 18033-3:2010(E)

Contents

Page

Foreword v
1 Scope 1
2 Terms and definitions 1
3 Symbols 2
4 64-bit block ciphers 3
4.1 Introduction 3
4.2 TDEA 3
4.2.1 The Triple Data Encryption Algorithm 3
4.2.2 TDEA encryption/decryption 3
4.2.3 TDEA keying options 4
4.3 MISTY1 4
4.3.1 The MISTY1 algorithm 4
4.3.2 MISTY1 encryption 4
4.3.3 MISTY1 decryption 5
4.3.4 MISTY1 functions 5
4.3.5 MISTY1 key schedule 10
4.4 CAST-128 11
4.4.1 The CAST-128 algorithm 11
4.4.2 CAST-128 encryption 11
4.4.3 CAST-128 decryption 11
4.4.4 CAST-128 functions 11
4.4.5 CAST-128 key schedule 18
4.5 HIGHT 20
4.5.1 The HIGHT algorithm 20
4.5.2 HIGHT encryption 21
4.5.3 HIGHT decryption 22
4.5.4 HIGHT functions 23
4.5.5 HIGHT key schedule 23
5 128-bit block ciphers 24
5.1 Introduction 24
5.2 AES 24
5.2.1 The AES algorithm 24
5.2.2 AES encryption 24
5.2.3 AES decryption 25
5.2.4 AES transformations 26
5.2.5 AES key schedule 30
5.3 Camellia 32
5.3.1 The Camellia algorithm 32
5.3.2 Camellia encryption 32
5.3.3 Camellia decryption 34
5.3.4 Camellia functions 37
5.3.5 Camellia key schedule 43
5.4 SEED 47
5.4.1 The SEED algorithm 47
5.4.2 SEED encryption 47
5.4.3 SEED decryption 47
5.4.4 SEED functions 48
5.4.5 SEED key schedule 50
Annex A (normative) Description of DES 52

A.1 Introduction 52
A.2 DES encryption 52
A.3 DES decryption 52
A.4 DES functions 52
A.4.1 Initial permutation *IP* 52
A.4.2 Inverse initial permutation IP^{-1} 54
A.4.3 Function *f* 54
A.4.4 Expansion permutation *E* 55
A.4.5 Permutation *P* 55
A.4.6 S-Boxes 56
A.5 DES key schedule 57

Annex B (normative) Object identifiers 60

Annex C (informative) Algebraic forms of MISTY1 and Camellia S-boxes 62
C.1 Introduction 62
C.2 MISTY1 S-boxes 62
C.2.1 The S-boxes S_7 and S_9 62
C.2.2 MISTY1 S-box S_7 62
C.2.3 MISTY1 S-box S_9 62
C.3 Camellia S-boxes 63

Annex D (informative) Test vectors 64
D.1 Introduction 64
D.2 TDEA test vectors 64
D.2.1 TDEA encryption 64
D.2.2 DES encryption and decryption 65
D.3 MISTY1 test vectors 66
D.4 CAST-128 test vectors 67
D.5 HIGHT test vectors 67
D.6 AES test vectors 67
D.6.1 AES encryption 67
D.6.2 Key expansion example 68
D.6.3 Cipher example 70
D.7 Camellia test vectors 73
D.7.1 Introduction 73
D.7.2 Camellia encryption 73
D.8 SEED test vectors 75

Annex E (informative) Feature table 77

Bibliography 78

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 18033-3 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 18033-3:2005), which has been technically revised. It also incorporates the Technical Corrigenda ISO/IEC 18033-3:2005/Cor.1:2006, ISO/IEC 18033-3:2005/Cor.2:2007 and ISO/IEC 18033-3:2005/Cor.3:2008.

ISO/IEC 18033 consists of the following parts, under the general title *Information technology — Security techniques — Encryption algorithms*:

— *Part 1: General*

— *Part 2: Asymmetric ciphers*

— *Part 3: Block ciphers*

— *Part 4: Stream ciphers*

Information technology — Security techniques — Encryption algorithms —

Part 3: **Block ciphers**

1 Scope

This part of ISO/IEC 18033 specifies block ciphers. A block cipher maps blocks of *n* bits to blocks of *n* bits, under the control of a key of *k* bits. A total of seven different block ciphers are defined. They are categorized in Table 1.

Table 1 — Block ciphers specified

Block length	Algorithm name	(see #)	Key length
64 bits	TDEA	(4.2)	128 or 192 bits
	MISTY1	(4.3)	128 bits
	CAST-128	(4.4)	
	HIGHT	(4.5)	
128 bits	AES	(5.2)	128, 192 or 256 bits
	Camellia	(5.3)	
	SEED	(5.4)	128 bits

The algorithms specified in this part of ISO/IEC 18033 have been assigned object identifiers in accordance with ISO/IEC 9834. The list of assigned object identifiers is given in Annex B. Any changes to the specification of the algorithms resulting in a change of functional behaviour will result in a change of the object identifier assigned to the algorithm.

2 Terms and definitions

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

2.1
block
string of bits of defined length

NOTE In this part of ISO/IEC 18033, the block length is either 64 or 128 bits.

[ISO/IEC 18033-1:2005]

2.2
block cipher
symmetric encipherment system with the property that the encryption algorithm operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext

[ISO/IEC 18033-1:2005]

2.3
ciphertext
data which has been transformed to hide its information content

[ISO/IEC 9798-1:1997]

2.4
key
sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment)

NOTE In all the ciphers specified in this part of ISO/IEC 18033, keys consist of a sequence of bits.

[ISO/IEC 11770-1:1996]

2.5
***n*-bit block cipher**
block cipher with the property that plaintext blocks and ciphertext blocks are *n* bits in length

[ISO/IEC 10116:2006]

2.6
plaintext
unenciphered information

[ISO/IEC 9797-1:1999]

3 Symbols

n plaintext/ciphertext bit length for a block cipher

E_K encryption function with key K

D_K decryption function with key K

Nr the number of rounds for the AES algorithm, which is 10, 12 or 14 for the choices of key length 128, 192 or 256 bits respectively

$\oplus$ the bit-wise logical exclusive-OR operation on bit-strings, i.e., if A, B are strings of the same length then $A \oplus B$ is the string equal to the bit-wise logical exclusive-OR of A and B

$\otimes$ multiplication of two polynomials (each with degree < 4) modulo $x^4 + 1$

$\wedge$ the bit-wise logical AND operation on bit-strings, i.e., if A, B are strings of the same length then $A \wedge B$ is the string equal to the bit-wise logical AND of A and B

$\vee$ the bit-wise logical OR operation on bit-strings, i.e., if A, B are strings of the same length then $A \vee B$ is the string equal to the bit-wise logical OR of A and B

|| concatenation of bit strings

• finite field multiplication

$<<<_i$ the left circular rotation of the operand by i bits

$>>>_i$ the right circular rotation of the operand by i bits

$\overline{x}$ the bitwise complement of x

a mod n for integers a and n, (a mod n) denotes the (non-negative) remainder obtained when a is divided by n. Equivalently if $b = a$ mod n, then b is the unique integer satisfying:
(i) $0 \leq b < n$, and
(ii) $(b-a)$ is an integer multiple of n

⊞ addition in modular arithmetic, i.e., if A, B are t-bit strings then $A⊞B$ is defined to equal ($A+B$ *mod* 2^t)

⊟ subtraction in modular arithmetic, i.e., if A, B are t-bit strings then $A⊟B$ is defined to equal ($A-B$ *mod* 2^t)

4 64-bit block ciphers

4.1 Introduction

In this clause, four 64-bit block ciphers are specified; TDEA (or ‘Triple DES’) in 4.2, MISTY1 in 4.3, CAST-128 in 4.4, and HIGHT in 4.5.

Users authorized to access data that has been enciphered shall have the key that was used to encipher the data in order to decipher it. The algorithm for any cipher in this clause is designed to encipher and decipher blocks of data consisting of 64 bits under control of a 128- (or 192-) bit key. Deciphering shall be accomplished using the same key as for enciphering.

4.2 TDEA

4.2.1 The Triple Data Encryption Algorithm

The Triple Data Encryption Algorithm (TDEA) is a symmetric cipher that can process data blocks of 64 bits, using cipher keys with length of 128 (or 192) bits, of which 112 (or 168) bits can be chosen arbitrarily, and the rest may be used for error detection. The TDEA is commonly known as Triple DES (Data Encryption Standard).

A TDEA encryption/decryption operation is a compound operation of DES encryption and decryption operations, where the DES algorithm is specified in Annex A. A TDEA key consists of three DES keys.

4.2.2 TDEA encryption/decryption

4.2.2.1 Encryption/decryption definitions

The TDEA is defined in terms of DES operations, where E_K is the DES encryption operation for the key K and D_K is the DES decryption operation for the key K.

4.2.2.2 TDEA encryption

The transformation of a 64-bit block P into a 64-bit block C is defined as follows:

$$C = E_{K_3}(D_{K_2}(E_{K_1}(P))).$$

4.2.2.3 TDEA decryption

The transformation of a 64-bit block C into a 64-bit block P is defined as follows:

$$P = D_{K_1}(E_{K_2}(D_{K_3}(C))).$$

4.2.3 TDEA keying options

This part of ISO/IEC 18033 specifies the following keying options for TDEA. The TDEA key comprises the triple (K_1, K_2, K_3).

1. Keying Option 1: K_1, K_2 and K_3 are different DES keys;

2. Keying Option 2: K_1 and K_2 are different DES keys and $K_3 = K_1$.

NOTE The option that $K_1 = K_2 = K_3$, the single-DES equivalent, is not recommended. Furthermore, the use of keying option 1 is preferred over keying option 2 since it provides additional security at the same performance level (see [3] for further details).

4.3 MISTY1

4.3.1 The MISTY1 algorithm

The MISTY1 algorithm is a symmetric block cipher that can process data blocks of 64 bits, using a cipher key with length of 128 bits.

4.3.2 MISTY1 encryption

The encryption operation is as shown in Figure 1. The transformation of a 64-bit block P into a 64-bit block C is defined as follows (KL, KO and KI are keys):

(1) $P = L_0 \| R_0$

$KL = KL_1 \| KL_2 \| \ldots \| KL_{10}$

$KO = KO_1 \| KO_2 \| \ldots \| KO_8$

$KI = KI_1 \| KI_2 \| \ldots \| KI_8$

(2) for i = 1, 3, …, 7 (increment in steps of 2 because the loop body consists of two rounds):

$R_i = \mathrm{FL}(L_{i-1}, KL_i)$

$L_i = \mathrm{FL}(R_{i-1}, KL_{i+1}) \oplus \mathrm{FO}(R_i, KO_i, KI_i)$

$L_{i+1} = R_i \oplus \mathrm{FO}(L_i, KO_{i+1}, KI_{i+1})$

$R_{i+1} = L_i$

for i = 9:

$R_i = \mathrm{FL}(L_{i-1}, KL_i)$

$L_i = \mathrm{FL}(R_{i-1}, KL_{i+1})$

(3) $C = L_9 \| R_9$

4.3.3 MISTY1 decryption

The decryption operation is as shown in Figure 2, and is identical in operation to encryption apart from the following two modifications.

(1) All FL functions are replaced by their inverse functions FL^{-1}.

(2) The order in which the subkeys are applied is reversed.

4.3.4 MISTY1 functions

4.3.4.1 MISTY1 function definitions

The MISTY1 algorithm uses a number of functions, namely S_7, S_9, FI, FO, FL and FL^{-1}, which are now defined.

4.3.4.2 Function FL

The FL function is used in encryption only and is shown in Figure 3. The FL function is defined as follows (*X* and *Y* are data, *KL* is a key):

(1) $X_{32} = X_L \parallel X_R$, $KL_i = KL_{iL} \parallel KL_{iR}$

(2) $Y_R = (X_L \wedge KL_{iL}) \oplus X_R$

(3) $Y_L = X_L \oplus (Y_R \vee KL_{iR})$

(4) $Y_{32} = Y_L \parallel Y_R$

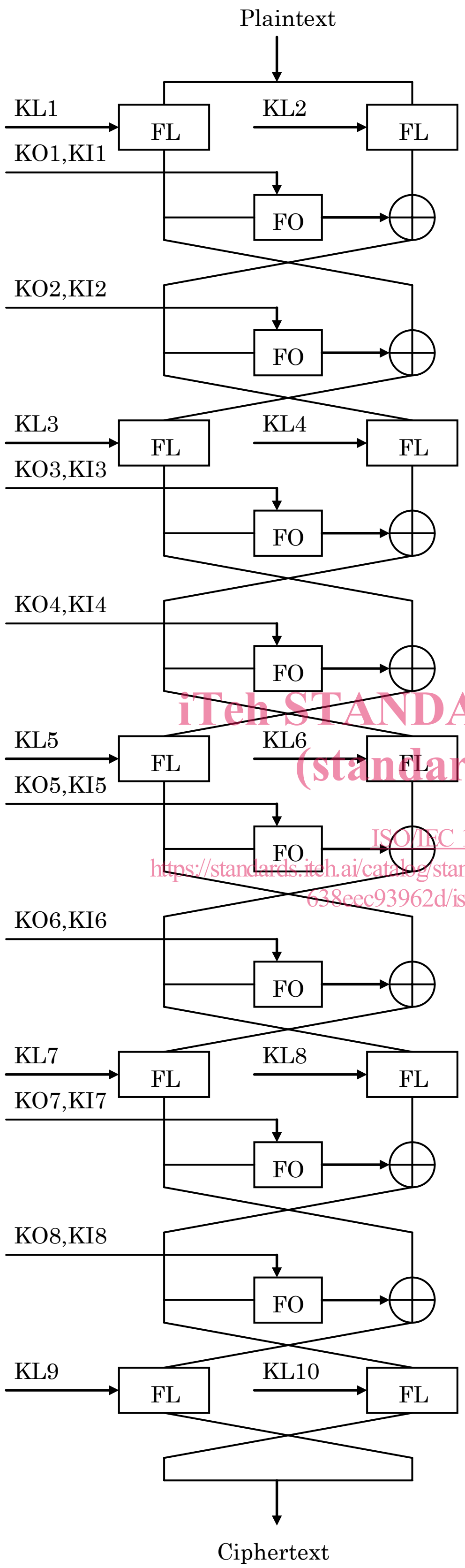

Figure 1 — The Encryption Procedure

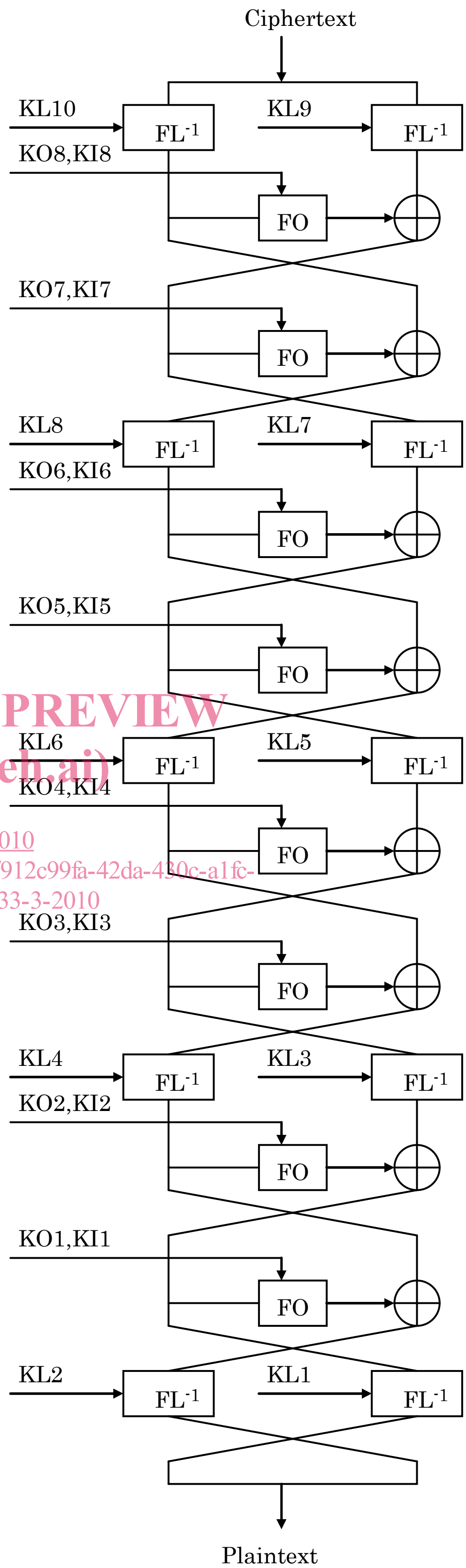

Figure 2 — The Decryption Procedure

4.3.4.3 Function FL^{-1}

The FL^{-1} function, which is the inverse to the FL function, is used in decryption only and is shown in Figure 4. The FL^{-1} function is defined as follows (X and Y are data, KL is a key):

(1) $Y_{32} = Y_L \,||\, Y_R$, $KL_i = KL_{iL} \,||\, KL_{iR}$

(2) $X_L = Y_L \oplus (Y_R \vee KL_{iR})$

(3) $X_R = (X_L \wedge KL_{iL}) \oplus Y_R$

(4) $X_{32} = X_L \,||\, X_R$

4.3.4.4 Function FO

The FO function is used in encryption and decryption, and is shown in Figure 5. The FO function is defined as follows (X and Y are data, KO and KI are keys):

(1) $X_{32} = L_0 \,||\, R_0$

$KO_i = KO_{i1} \,||\, KO_{i2} \,||\, KO_{i3} \,||\, KO_{i4}$, $KI_i = KI_{i1} \,||\, KI_{i2} \,||\, KI_{i3}$

(2) for j = 1 to 3 :

$R_j = \mathrm{FI}(L_{j-1} \oplus KO_{ij}, KI_{ij}) \oplus R_{j-1}$

$L_j = R_{j-1}$

(3) $Y_{32} = (L_3 \oplus KO_{i4}) \,||\, R_3$

4.3.4.5 Function FI

The FI function is used for encryption, decryption and the key schedule, and is shown in Figure 6, where Extnd is the operation zero-extended from 7 bits to 9 bits by the concatenation of two bits on the left side, and Trunc is the operation truncated by two bits on the left side. The FI function is defined as follows (X and Y are data, KI is a key):

(1) $X_{16} = L_0$ (9 bits) $||$ R_0 (7 bits), $KI_{ij} = KI_{ijL} \,||\, KI_{ijR}$

(2) $R_1 = \mathrm{S}_9(L_0) \oplus \mathrm{Extnd}(R_0)$

(3) $L_1 = R_0$

(4) $R_2 = \mathrm{S7}(L_1) \oplus \mathrm{Trunc}(R_1) \oplus KI_{ijL}$

(5) $L_2 = R_1 \oplus KI_{ijR}$

(6) $R_3 = \mathrm{S}_9(L_2) \oplus \mathrm{Extnd}(R_2)$

(7) $L_3 = R_2$

(8) $Y_{16} = L_3 \,||\, R_3$

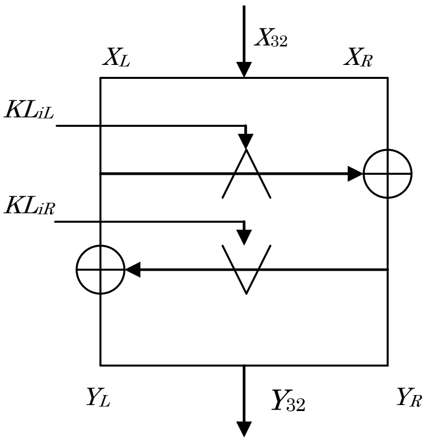

Figure 3 — The Function FL

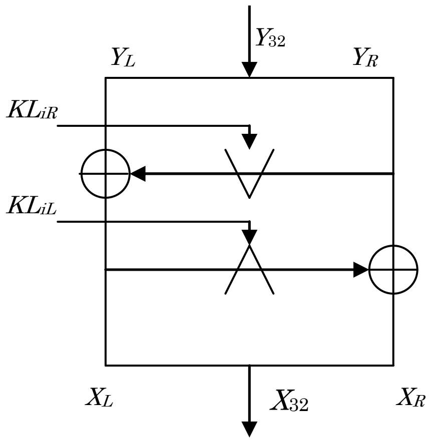

Figure 4 — The Function FL^{-1}

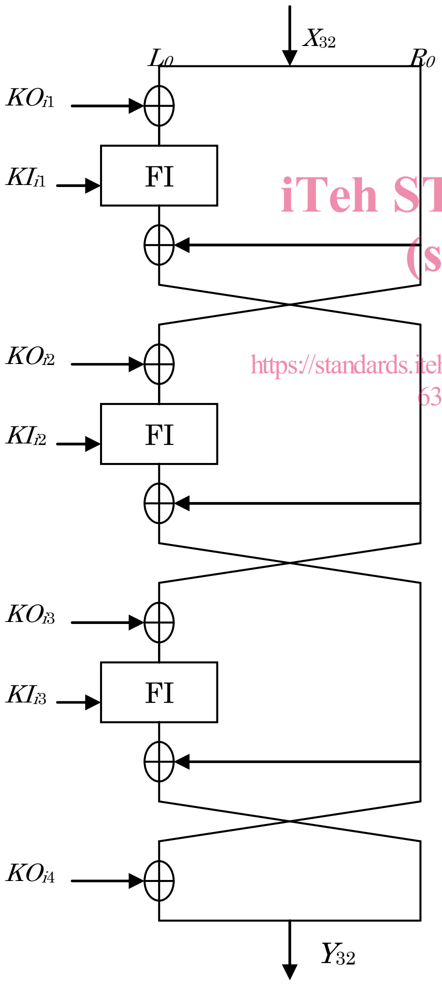

Figure 5 — The Function FO

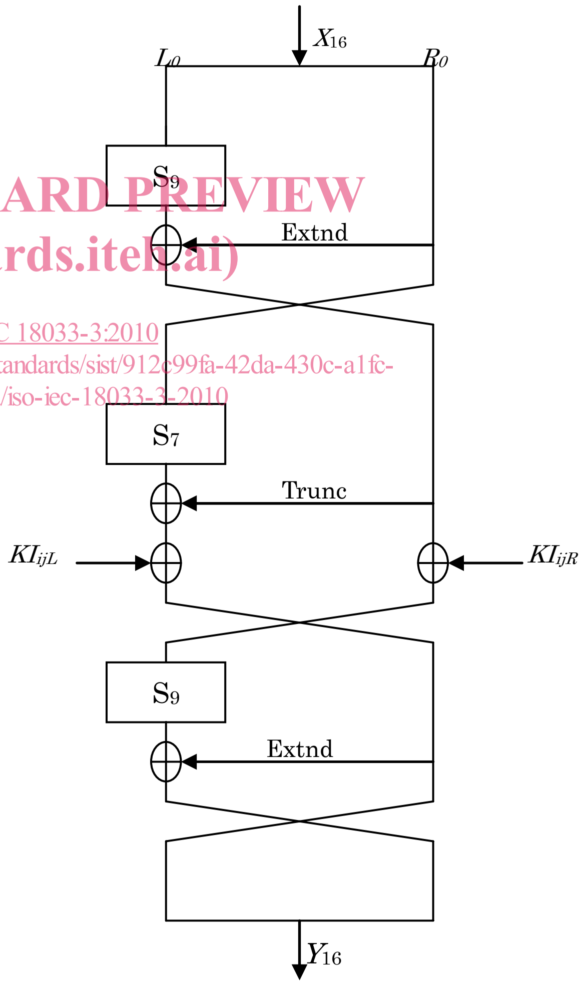

Figure 6 — The Function FI

4.3.4.6 Lookup Tables S_7 and S_9

S_7 is a bijective lookup table that accepts a 7-bit input and yields a 7-bit output. S_9 is a bijective lookup table that accepts a 9-bit input and yields a 9-bit output. Tables 2 and 3 define these lookup tables in a hexadecimal form. S_7 and S_9 can be also described in a simple algebraic form over GF(2) as shown in clause C.2.

For example, if the input to S_7 is {53}, then the substitution value would be determined by the intersection of the row with index '5' and the column with index '3' in Table 2. This would result in S_7 having a value of {57}.

Table 2 — S_7

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	1b	32	33	5a	3b	10	17	54	5b	1a	72	73	6b	2c	66	49
1	1f	24	13	6c	37	2e	3f	4a	5d	0f	40	56	25	51	1c	04
2	0b	46	20	0d	7b	35	44	42	2b	1e	41	14	4b	79	15	6f
3	0e	55	09	36	74	0c	67	53	28	0a	7e	38	02	07	60	29
4	19	12	65	2f	30	39	08	68	5f	78	2a	4c	64	45	75	3d
5	59	48	03	57	7c	4f	62	3c	1d	21	5e	27	6a	70	4d	3a
6	01	6d	6e	63	18	77	23	05	26	76	00	31	2d	7a	7f	61
7	50	22	11	06	47	16	52	4e	71	3e	69	43	34	5c	58	7d

Table 3 — S_9

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
00	1c3	0cb	153	19f	1e3	0e9	0fb	035	181	0b9	117	1eb	133	009	02d	0d3
01	0c7	14a	037	07e	0eb	164	193	1d8	0a3	11e	055	02c	01d	1a2	163	118
02	14b	152	1d2	00f	02b	030	13a	0e5	111	138	18e	063	0e3	0c8	1f4	01b
03	001	09d	0f8	1a0	16d	1f3	01c	146	07d	0d1	082	1ea	183	12d	0f4	19e
04	1d3	0dd	1e2	128	1e0	0ec	059	091	011	12f	026	0dc	0b0	18c	10f	1f7
05	0e7	16c	0b6	0f9	0d8	151	101	14c	103	0b8	154	12b	1ae	017	071	00c
06	047	058	07f	1a4	134	129	084	15d	19d	1b2	1a3	048	07c	051	1ca	023
07	13d	1a7	165	03b	042	0da	192	0ce	0c1	06b	09f	1f1	12c	184	0fa	196
08	1e1	169	17d	031	180	10a	094	1da	186	13e	11c	060	175	1cf	067	119
09	065	068	099	150	008	007	17c	0b7	024	019	0de	127	0db	0e4	1a9	052
0a	109	090	19c	1c1	028	1b3	135	16a	176	0df	1e5	188	0c5	16e	1de	1b1
0b	0c3	1df	036	0ee	1ee	0f0	093	049	09a	1b6	069	081	125	00b	05e	0b4
0c	149	1c7	174	03e	13b	1b7	08e	1c6	0ae	010	095	1ef	04e	0f2	1fd	085
0d	0fd	0f6	0a0	16f	083	08a	156	09b	13c	107	167	098	1d0	1e9	003	1fe
0e	0bd	122	089	0d2	18f	012	033	06a	142	0ed	170	11b	0e2	14f	158	131
0f	147	05d	113	1cd	079	161	1a5	179	09e	1b4	0cc	022	132	01a	0e8	004
10	187	1ed	197	039	1bf	1d7	027	18b	0c6	09c	0d0	14e	06c	034	1f2	06e
11	0ca	025	0ba	191	0fe	013	106	02f	1ad	172	1db	0c0	10b	1d6	0f5	1ec
12	10d	076	114	1ab	075	10c	1e4	159	054	11f	04b	0c4	1be	0f7	029	0a4
13	00e	1f0	077	04d	17a	086	08b	0b3	171	0bf	10e	104	097	15b	160	168

