

---

---

**Information security — Lightweight  
cryptography —**

**Part 2:  
Block ciphers**

*Sécurité de l'information — Cryptographie pour environnements  
contraints —*

*Partie 2: Chiffrements par blocs*

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 29192-2:2019



STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 29192-2:2019



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2019

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Phone: +41 22 749 01 11  
Fax: +41 22 749 09 47  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

|  | Page      |
|--|-----------|
| Foreword .....   | iv        |
| Introduction .....   | v         |
| <b>1 Scope</b> .....   | <b>1</b>  |
| <b>2 Normative references</b> .....  | <b>1</b>  |
| <b>3 Terms and definitions</b> .....   | <b>1</b>  |
| <b>4 Symbols</b> .....   | <b>2</b>  |
| <b>5 Lightweight block cipher with a block size of 64 bits</b> .....                 | <b>2</b>  |
| 5.1 General .....  | 2         |
| 5.2 PRESENT .....  | 2         |
| 5.2.1 PRESENT algorithm .....  | 2         |
| 5.2.2 PRESENT specific notation .....  | 2         |
| 5.2.3 PRESENT encryption .....   | 3         |
| 5.2.4 PRESENT decryption .....   | 4         |
| 5.2.5 PRESENT transformations .....  | 4         |
| 5.2.6 PRESENT key schedule .....   | 5         |
| <b>6 Lightweight block ciphers with a block size of 128 bits</b> .....               | <b>7</b>  |
| 6.1 General .....  | 7         |
| 6.2 CLEFIA .....   | 7         |
| 6.2.1 CLEFIA algorithm .....   | 7         |
| 6.2.2 CLEFIA specific notation .....   | 7         |
| 6.2.3 CLEFIA encryption .....  | 7         |
| 6.2.4 CLEFIA decryption .....  | 8         |
| 6.2.5 CLEFIA building blocks .....   | 9         |
| 6.2.6 CLEFIA key schedule .....  | 14        |
| 6.3 LEA .....  | 24        |
| 6.3.1 LEA algorithm .....  | 24        |
| 6.3.2 LEA specific notation .....  | 24        |
| 6.3.3 LEA encryption .....   | 24        |
| 6.3.4 LEA decryption .....   | 26        |
| 6.3.5 LEA key schedule .....   | 27        |
| <b>Annex A (normative) Object identifiers</b> .....                                  | <b>30</b> |
| <b>Annex B (informative) Numerical examples</b> .....                                | <b>31</b> |
| <b>Annex C (informative) Feature tables</b> .....                                    | <b>53</b> |
| <b>Annex D (informative) A limitation of a block cipher under a single key</b> ..... | <b>55</b> |
| <b>Bibliography</b> .....  | <b>56</b> |

## 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](http://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 and IEC shall not be held responsible for identifying any of 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](http://www.iso.org/patents)) or the IEC list of patent declarations received (see <http://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](http://www.iso.org/iso/foreword.html).

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](http://www.iso.org/members.html).

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

This second edition cancels and replaces the first edition (ISO/IEC 29192-2:2012), which has been technically revised.

The main changes compared to the previous edition are as follows:

- the LEA algorithm has been added to [6.3](#);
- numerical examples and feature tables of LEA have been added to [B.3](#) and [Annex C](#).

A list of all parts in the ISO/IEC 29192 series can be found on the ISO website.

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](http://www.iso.org/members.html).

## Introduction

ISO/IEC 29192-1 specifies the requirements for lightweight cryptography.

A block cipher maps blocks of  $n$  bits to blocks of  $n$  bits, under the control of a key of  $k$  bits.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of a patent.

ISO and IEC takes no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured ISO and IEC that he/she is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO and IEC. Information may be obtained from the patent database available at [www.iso.org/patents](http://www.iso.org/patents).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those in the patent database. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 29192-2:2019

# Information security — Lightweight cryptography —

## Part 2: Block ciphers

### 1 Scope

This document specifies three block ciphers suitable for applications requiring lightweight cryptographic implementations:

- PRESENT: a lightweight block cipher with a block size of 64 bits and a key size of 80 or 128 bits;
- CLEFIA: a lightweight block cipher with a block size of 128 bits and a key size of 128, 192 or 256 bits;
- LEA: a lightweight block cipher with a block size of 128 bits and a key size of 128, 192 or 256 bits.

### 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 terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

#### 3.1

##### **block**

string of bits of defined length

[SOURCE: ISO/IEC 18033-1:2015, 2.8]

#### 3.2

##### **block cipher**

symmetric encipherment system with the property that the encryption algorithm operates on a *block* (3.1) of *plaintext* (3.6), i.e. a string of bits of a defined length, to yield a block of *ciphertext* (3.3)

[SOURCE: ISO/IEC 18033-1:2015, 2.9]

#### 3.3

##### **ciphertext**

data which has been transformed to hide its information content

[SOURCE: ISO/IEC 10116:2017, 3.2]

#### 3.4

##### **key**

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

[SOURCE: ISO/IEC 18033-1:2015, 2.27]

**3.5**  
***n*-bit block cipher**

*block cipher* (3.2) with the property that *plaintext* (3.6) blocks and *ciphertext* (3.3) blocks are *n* bits in length

[SOURCE: ISO/IEC 18033-1:2015, 2.29]

**3.6**  
**plaintext**  
unenciphered information

[SOURCE: ISO/IEC 9798-1:2010, 3.19]

**3.7**  
**round key**  
sequence of symbols derived from the *key* (3.4) using the key schedule, and used to control the transformation in each round of the *block cipher* (3.2)

**4 Symbols**

$0\times$  a prefix for a binary string in hexadecimal notation

$\parallel$  concatenation of bit strings

$a \leftarrow b$  updating a value of *a* by a value of *b*

$\oplus$  bitwise exclusive-OR operation

**5 Lightweight block cipher with a block size of 64 bits**

**5.1 General**

In this clause, a 64-bit lightweight block cipher is specified: PRESENT in 5.2.

[Annex A](#) defines the object identifiers which shall be used to identify the algorithm specified in [Clause 5](#). [Annex B](#) provides numerical examples of the block ciphers described in this document. [Annex C](#) summarizes the lightweight properties of the block ciphers described in this document. [Annex D](#) gives a limit on the number of block cipher encryption operations that should be performed using a single key.

**5.2 PRESENT**

**5.2.1 PRESENT algorithm**

The PRESENT algorithm<sup>[10]</sup> is a symmetric block cipher that can process data blocks of 64 bits, using a key of length 80 or 128 bits. The cipher is referred to as PRESENT-80 or PRESENT-128 when using an 80-bit or 128-bit key respectively.

**5.2.2 PRESENT specific notation**

$K_i = k_{63}^i \dots k_0^i$  64-bit round key that is used in round *i*

$k_b^i$  bit *b* of round key  $K_i$

$K = k_{79} \dots k_0$  80-bit key register

$k_b$  bit *b* of key register  $K$

*STATE* 64-bit internal state  
*b<sub>i</sub>* bit *i* of the current *STATE*  
*w<sub>i</sub>* 4-bit word where  $0 \leq i \leq 15$

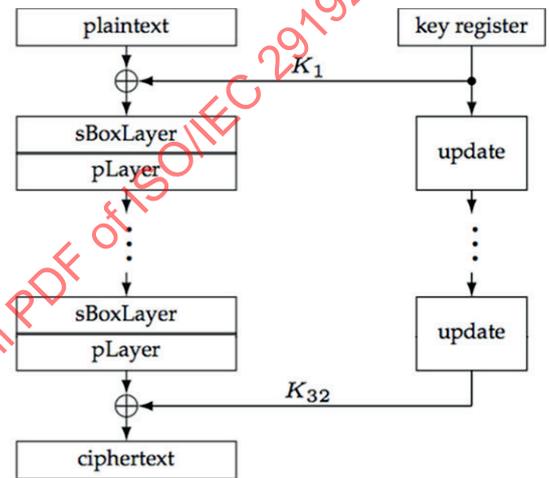
**5.2.3 PRESENT encryption**

The PRESENT block cipher consists of 31 "rounds", i.e. 31 applications of a sequence of simple transformations. A pseudocode description of the complete encryption algorithm is provided in Figure 1, where *STATE* denotes the internal state. The individual transformations used by the algorithm are defined in 5.2.5. Each round of the algorithm uses a distinct round key  $K_i$  ( $1 \leq i \leq 31$ ), derived as specified in 5.2.6. Two consecutive rounds of the algorithm are shown for illustrative purposes in Figure 2.

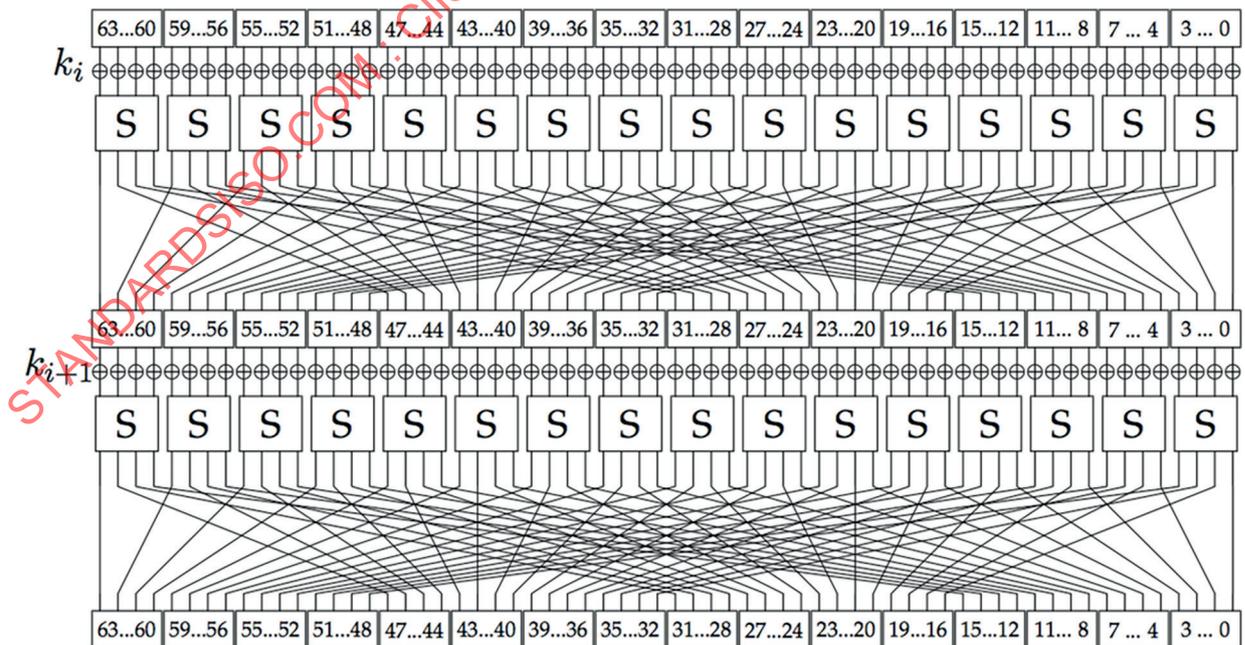
```

generateRoundKeys()
for i = 1 to 31 do

    addRoundKey(STATE,  $K_i$ )
    sBoxLayer(STATE)
    pLayer(STATE)
end for
addRoundKey(STATE,  $K_{32}$ )
    
```



**Figure 1 — The encryption procedure of PRESENT**



**Figure 2 — Two rounds of PRESENT**

5.2.4 PRESENT decryption

The complete PRESENT decryption algorithm is given in Figure 3. The individual transformations used by the algorithm are defined in 5.2.5. Each round of the algorithm uses a distinct round key  $K_i$  ( $1 \leq i \leq 31$ ), derived as specified in 5.2.6.

```

generateRoundKeys()
addRoundKey(STATE, K32)
for i = 31 downto 1 do
    invpLayer(STATE)
    invsBoxLayer(STATE)

    addRoundKey(STATE, Ki)
end for
    
```

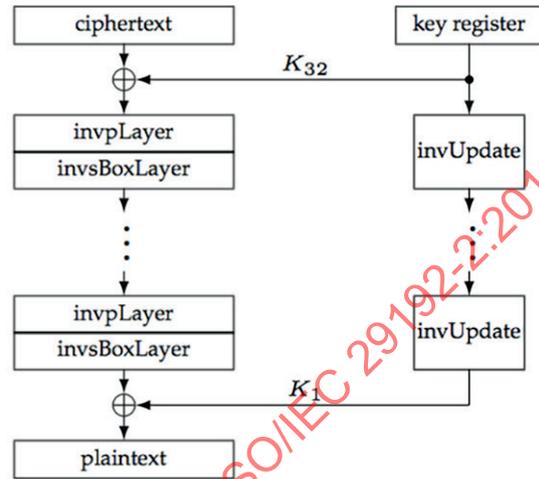


Figure 3 — The decryption procedure of PRESENT

5.2.5 PRESENT transformations

5.2.5.1 addRoundKey

Given round key  $K_i = k_{63}^i \dots k_0^i$  for  $1 \leq i \leq 32$  and current STATE  $b_{63} \dots b_0$ , **addRoundKey** consists of the operation for  $0 \leq j \leq 63$ ,  $b_j \leftarrow b_j \oplus k_j^i$ .

5.2.5.2 sBoxLayer

The non-linear **sBoxLayer** of the encryption process of PRESENT uses a single 4-bit to 4-bit S-box  $S$  which is applied 16 times in parallel in each round. The S-box transforms the input  $x$  to an output  $S(x)$  as given in hexadecimal notation in Table 1.

Table 1 — PRESENT S-box

| $x$    | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|--------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $S(x)$ | C | 5 | 6 | B | 9 | 0 | A | D | 3 | E | F | 8 | 4 | 7 | 1 | 2 |

For **sBoxLayer** the current STATE  $b_{63} \dots b_0$  is considered as sixteen 4-bit words  $w_{15} \dots w_0$  where  $w_i = b_{4*i+3} \parallel b_{4*i+2} \parallel b_{4*i+1} \parallel b_{4*i}$  for  $0 \leq i \leq 15$  and the output nibble  $S(w_i)$  provides the updated state values as a concatenation  $S(w_{15}) \parallel S(w_{14}) \parallel \dots \parallel S(w_0)$ .

5.2.5.3 invsBoxLayer

The S-box used in the decryption procedure of PRESENT is the inverse of the 4-bit to 4-bit S-box  $S$  that is described in 5.2.5.2. The inverse S-box transforms the input  $x$  to an output  $S^{-1}(x)$  as given in hexadecimal notation in Table 2.

Table 2 — PRESENT inverse S-box

| $x$         | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|-------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $S^{-1}(x)$ | 5 | E | F | 8 | C | 1 | 2 | D | B | 4 | 6 | 3 | 0 | 7 | 9 | A |

### 5.2.5.4 pLayer

The bit permutation **pLayer** used in the encryption routine of PRESENT is given by [Table 3](#). Bit  $i$  of *STATE* is moved to bit position  $P(i)$ .

**Table 3 — PRESENT permutation layer pLayer**

|        |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|--------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| $i$    | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 | 11 | 12 | 13 | 14 | 15 |
| $P(i)$ | 0  | 16 | 32 | 48 | 1  | 17 | 33 | 49 | 2  | 18 | 34 | 50 | 3  | 19 | 35 | 51 |
| $i$    | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| $P(i)$ | 4  | 20 | 36 | 52 | 5  | 21 | 37 | 53 | 6  | 22 | 38 | 54 | 7  | 23 | 39 | 55 |
| $i$    | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 |
| $P(i)$ | 8  | 24 | 40 | 56 | 9  | 25 | 41 | 57 | 10 | 26 | 42 | 58 | 11 | 27 | 43 | 59 |
| $i$    | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 |
| $P(i)$ | 12 | 28 | 44 | 60 | 13 | 29 | 45 | 61 | 14 | 30 | 46 | 62 | 15 | 31 | 47 | 63 |

### 5.2.5.5 invpLayer

The inverse permutation layer **invpLayer** used in the decryption routine of PRESENT is given by [Table 4](#). Bit  $i$  of *STATE* is moved to bit position  $P^{-1}(i)$ .

**Table 4 — PRESENT inverse permutation Layer invpLayer**

|             |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|-------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| $i$         | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 | 11 | 12 | 13 | 14 | 15 |
| $P^{-1}(i)$ | 0  | 4  | 8  | 12 | 16 | 20 | 24 | 28 | 32 | 36 | 40 | 44 | 48 | 52 | 56 | 60 |
| $i$         | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| $P^{-1}(i)$ | 1  | 5  | 9  | 13 | 17 | 21 | 25 | 29 | 33 | 37 | 41 | 45 | 49 | 53 | 57 | 61 |
| $i$         | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 |
| $P^{-1}(i)$ | 2  | 6  | 10 | 14 | 18 | 22 | 26 | 30 | 34 | 38 | 42 | 46 | 50 | 54 | 58 | 62 |
| $i$         | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 |
| $P^{-1}(i)$ | 3  | 7  | 11 | 15 | 19 | 23 | 27 | 31 | 35 | 39 | 43 | 47 | 51 | 55 | 59 | 63 |

## 5.2.6 PRESENT key schedule

### 5.2.6.1 PRESENT-80 and PRESENT-128

PRESENT can take keys of either 80 or 128 bits. In [5.2.6.2](#), the version with an 80-bit key (PRESENT-80) and in [5.2.6.3](#) the 128-bit version (PRESENT-128) is described.

5.2.6.2 80-bit key for PRESENT-80

The user-supplied key is stored in a key register  $K$  and represented as  $k_{79}k_{78} \dots k_0$ . At round  $i$  the 64-bit round key  $K_i = k_{63}^i k_{62}^i \dots k_0^i$  consists of the 64 leftmost bits of the current contents of register  $K$ . Thus at round  $i$ ,  $K_i$  is as follows:

$$K_i = k_{63}^i k_{62}^i \dots k_0^i = k_{79} k_{78} \dots k_{16}$$

After extracting the round key  $K_i$ , the key register  $K = k_{79}k_{78} \dots k_0$  is updated as follows.

- 1)  $k_{79}k_{78} \dots k_1 k_0 \leftarrow k_{18}k_{17} \dots k_{20}k_{19}$
- 2)  $k_{79}k_{78}k_{77}k_{76} \leftarrow S[k_{79}k_{78}k_{77}k_{76}]$
- 3)  $k_{19}k_{18}k_{17}k_{16}k_{15} \leftarrow k_{19}k_{18}k_{17}k_{16}k_{15} \oplus \text{round\_counter}$

In words, the key register is rotated by 61 bit positions to the left, the left-most four bits are passed through the PRESENT S-box, and the *round\_counter* value  $i$  is exclusive-ORed with bits  $k_{19}k_{18}k_{17}k_{16}k_{15}$  of  $K$  where the least significant bit of *round\_counter* is on the right. The rounds are numbered from  $1 \leq i \leq 31$  and *round\_counter* =  $i$ . Figure 4 depicts the key schedule for PRESENT-80 graphically.

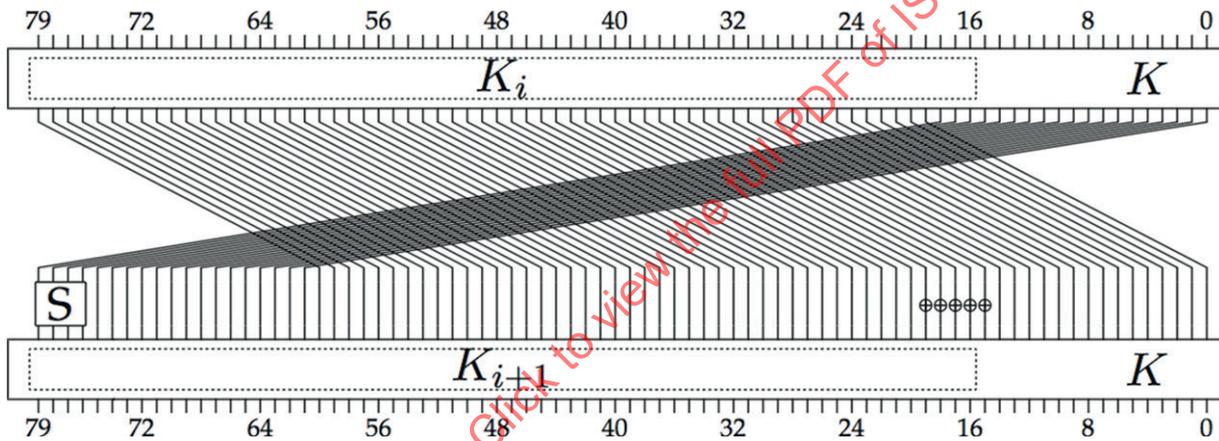


Figure 4 — PRESENT-80 key schedule

5.2.6.3 128-bit key for PRESENT-128

Similar to the 80-bit variant the user-supplied key is stored initially in a key register  $K$  and is represented as  $k_{127}k_{126} \dots k_0$ . At round  $i$  the 64-bit round key  $K_i = k_{63}^i k_{62}^i \dots k_0^i$  consists of the 64 leftmost bits of the current contents of register  $K$ . Thus at round  $i$ ,  $K_i$  is as follows:

$$K_i = k_{63}^i k_{62}^i \dots k_0^i = k_{127} k_{126} \dots k_{64}$$

After extracting the round key  $K_i$ , the key register  $K = k_{127}k_{126} \dots k_0$  is updated as follows.

- 1)  $k_{127}k_{126} \dots k_1 k_0 \leftarrow k_{66}k_{65} \dots k_{68}k_{67}$
- 2)  $k_{127}k_{126}k_{125}k_{124} \leftarrow S[k_{127}k_{126}k_{125}k_{124}]$
- 3)  $k_{123}k_{122}k_{121}k_{120} \leftarrow S[k_{123}k_{122}k_{121}k_{120}]$
- 4)  $k_{66}k_{65}k_{64}k_{63}k_{62} \leftarrow k_{66}k_{65}k_{64}k_{63}k_{62} \oplus \text{round\_counter}$

In words, the key register is rotated by 61 bit positions to the left, the left-most eight bits are passed through the PRESENT S-box, and the *round\_counter* value  $i$  is exclusive-ORed with bits  $k_{66}k_{65}k_{64}k_{63}k_{62}$

of  $K$  where the least significant bit of  $round\_counter$  is on the right. The rounds are numbered from  $1 \leq i \leq 31$  and  $round\_counter = i$ . Figure 5 depicts the key schedule for PRESENT-128 graphically.

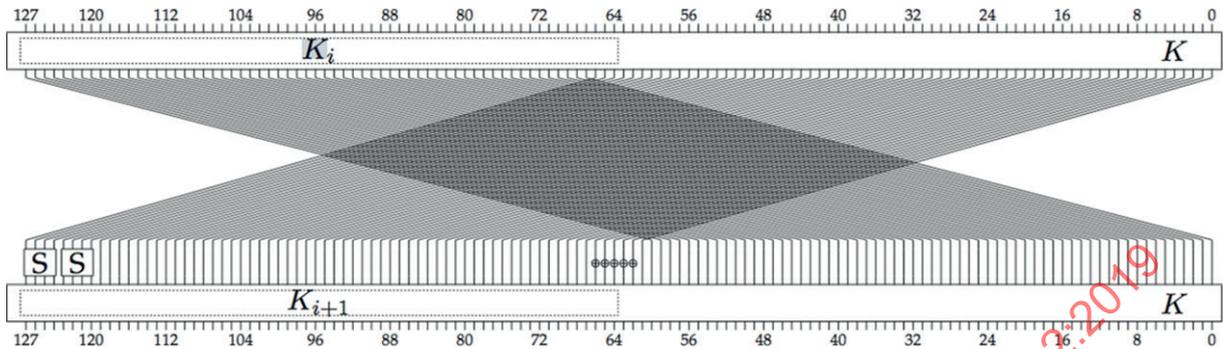


Figure 5 — PRESENT-128 key schedule

## 6 Lightweight block ciphers with a block size of 128 bits

### 6.1 General

In this clause, two 128-bit lightweight block ciphers are specified: CLEFIA in 6.2 and LEA in 6.3.

Annex A defines the object identifiers which shall be used to identify the algorithms specified in Clause 6. Annex B provides numerical examples of the block ciphers described in this document. Annex C summarizes the lightweight properties of the block ciphers described in this document. Annex D gives a limit on the number of block cipher encryption operations that should be performed using a single key.

### 6.2 CLEFIA

#### 6.2.1 CLEFIA algorithm

The CLEFIA algorithm<sup>[15]</sup> is a symmetric block cipher that can process data blocks of 128 bits using a cipher key of length 128, 192, or 256 bits. The number of rounds is 18, 22 and 26 for CLEFIA with 128-bit, 192-bit and 256-bit keys, respectively. The total number of round keys depends on the key length. The CLEFIA encryption and decryption functions require 36, 44 and 52 round keys for 128-bit, 192-bit and 256-bit keys, respectively.

#### 6.2.2 CLEFIA specific notation

|             |  |
|-------------|--|
| $a_{(b)}$   | bit string of bit length $b$                             |
| $\{0,1\}^n$ | a set of $n$ -bit binary strings                         |
| $\cdot$     | multiplication in $GF(2^n)$                              |
| $\lll i$    | $i$ -bit left cyclic shift operation                     |
| $\sim a$    | bitwise complement of bit string $a$                     |
| $\Sigma^n$  | $n$ times operations of the DoubleSwap function $\Sigma$ |

#### 6.2.3 CLEFIA encryption

The encryption process of CLEFIA is based on the 4-branch  $r$ -round generalized Feistel structure  $GFN_{4,r}$ . Let  $P, C \in \{0,1\}^{128}$  be a plaintext and a ciphertext. Let  $P_i, C_i \in \{0,1\}^{32}$  ( $0 \leq i < 4$ ) be divided plaintexts

and ciphertexts where  $P = P_0 \parallel P_1 \parallel P_2 \parallel P_3$  and  $C = C_0 \parallel C_1 \parallel C_2 \parallel C_3$ . Let  $WK_0, WK_1, WK_2, WK_3 \in \{0,1\}^{32}$  be whitening keys and  $RK_i \in \{0,1\}^{32}$  ( $0 \leq i < 2r$ ) be round keys provided by the key schedule. Then,  $r$ -round encryption function  $ENC_r$  is defined as follows:

$ENC_r$ :

- 1)  $T_0 \parallel T_1 \parallel T_2 \parallel T_3 \leftarrow P_0 \parallel (P_1 \oplus WK_0) \parallel P_2 \parallel (P_3 \oplus WK_1)$
- 2)  $T_0 \parallel T_1 \parallel T_2 \parallel T_3 \leftarrow GFN_{4,r}(RK_0, \dots, RK_{2r-1}, T_0, T_1, T_2, T_3)$
- 3)  $C_0 \parallel C_1 \parallel C_2 \parallel C_3 \leftarrow T_0 \parallel (T_1 \oplus WK_2) \parallel T_2 \parallel (T_3 \oplus WK_3)$

#### 6.2.4 CLEFIA decryption

The decryption function  $DEC_r$  is defined as follows:

$DEC_r$ :

- 1)  $T_0 \parallel T_1 \parallel T_2 \parallel T_3 \leftarrow C_0 \parallel (C_1 \oplus WK_2) \parallel C_2 \parallel (C_3 \oplus WK_3)$
- 2)  $T_0 \parallel T_1 \parallel T_2 \parallel T_3 \leftarrow GFN_{4,r}^{-1}(RK_0, \dots, RK_{2r-1}, T_0, T_1, T_2, T_3)$
- 3)  $P_0 \parallel P_1 \parallel P_2 \parallel P_3 \leftarrow T_0 \parallel (T_1 \oplus WK_0) \parallel T_2 \parallel (T_3 \oplus WK_1)$

[Figure 6](#) illustrates both  $ENC_r$  and  $DEC_r$ .

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 29192-2:2019

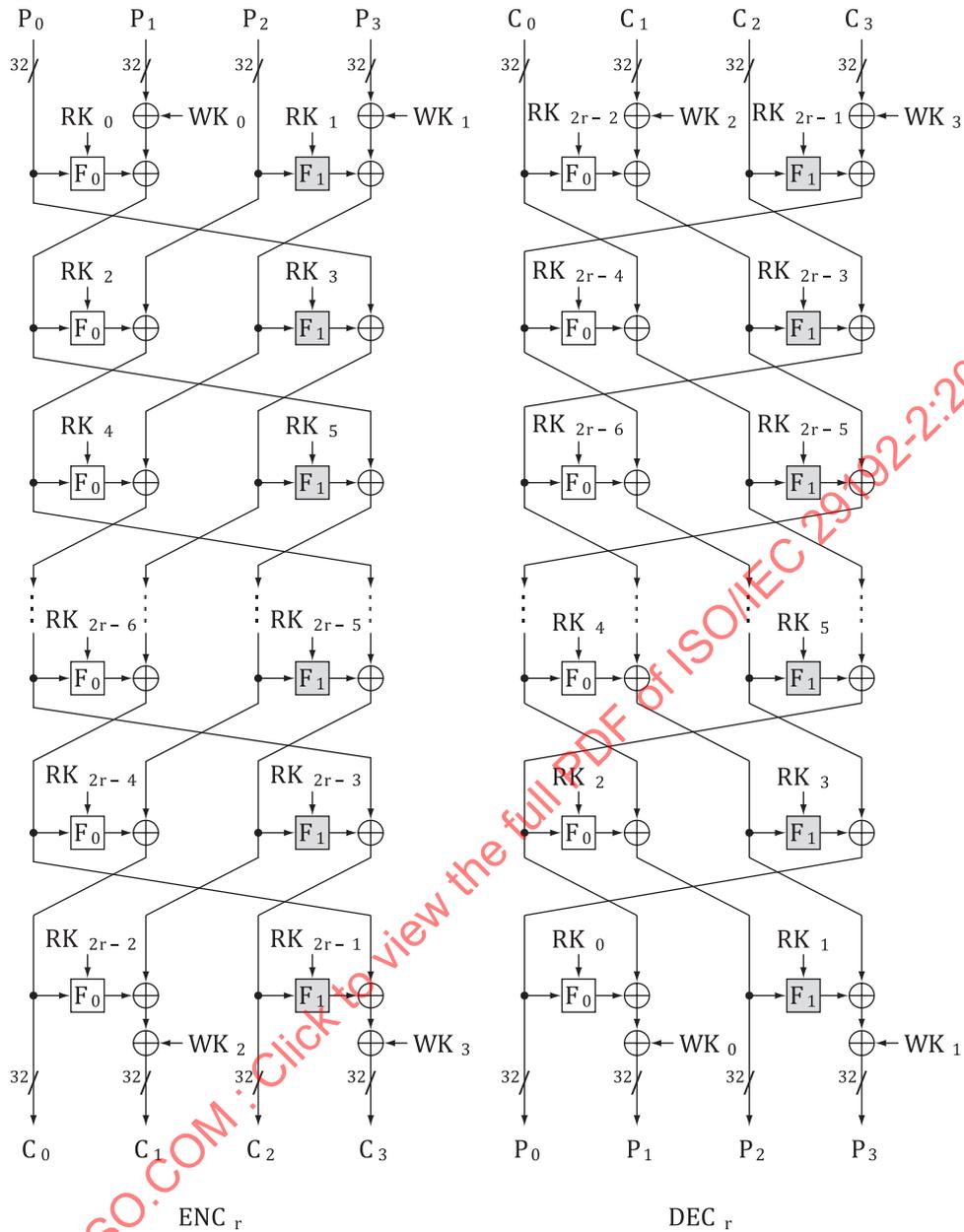


Figure 6 — The encryption procedure and the decryption procedure of CLEFIA

### 6.2.5 CLEFIA building blocks

#### 6.2.5.1 $GFN_{d,r}$

The fundamental structure of CLEFIA is a generalized Feistel structure. This structure is employed in both a data processing part and a key schedule part.

CLEFIA uses a 4-branch and an 8-branch generalized Feistel network. The 4-branch generalized Feistel network is used in the data processing part and the key schedule for a 128-bit key. The 8-branch generalized Feistel network is applied in the key schedule for a 192-bit/256-bit key. Let  $GFN_{d,r}$  denote the  $d$ -branch  $r$ -round generalized Feistel network employed in CLEFIA.  $GFN_{d,r}$  uses two different 32-bit F-functions  $F_0$  and  $F_1$ .

For  $d$  pairs of 32-bit input  $X_i$  and output  $Y_i$  ( $0 \leq i < d$ ), and  $dr/2$  32-bit round keys  $RK_i$  ( $0 \leq i < dr/2$ ),  $GFN_{d,r}$  ( $d = 4, 8$ ) and the inverse function  $GFN_{d,r}^{-1}$  ( $d = 4$ ) are defined as follows.

$GFN_{4,r}$ :

- 1)  $T_0 \parallel T_1 \parallel T_2 \parallel T_3 \leftarrow X_0 \parallel X_1 \parallel X_2 \parallel X_3$
- 2) For  $i = 0$  to  $r - 1$  do the following:
  - 2.1)  $T_1 \leftarrow T_1 \oplus F_0(RK_{2i}, T_0)$   
 $T_3 \leftarrow T_3 \oplus F_1(RK_{2i+1}, T_2)$
  - 2.2)  $T_0 \parallel T_1 \parallel T_2 \parallel T_3 \leftarrow T_1 \parallel T_2 \parallel T_3 \parallel T_0$
- 3)  $Y_0 \parallel Y_1 \parallel Y_2 \parallel Y_3 \leftarrow T_3 \parallel T_0 \parallel T_1 \parallel T_2$

$GFN_{8,r}$ :

- 1)  $T_0 \parallel T_1 \parallel \dots \parallel T_7 \leftarrow X_0 \parallel X_1 \parallel \dots \parallel X_7$
- 2) For  $i = 0$  to  $r - 1$  do the following:
  - 2.1)  $T_1 \leftarrow T_1 \oplus F_0(RK_{4i}, T_0)$   
 $T_3 \leftarrow T_3 \oplus F_1(RK_{4i+1}, T_2)$   
 $T_5 \leftarrow T_5 \oplus F_0(RK_{4i+2}, T_4)$   
 $T_7 \leftarrow T_7 \oplus F_1(RK_{4i+3}, T_6)$
  - 2.2)  $T_0 \parallel T_1 \parallel \dots \parallel T_6 \parallel T_7 \leftarrow T_1 \parallel T_2 \parallel \dots \parallel T_7 \parallel T_0$
- 3)  $Y_0 \parallel Y_1 \parallel \dots \parallel Y_6 \parallel Y_7 \leftarrow T_7 \parallel T_0 \parallel \dots \parallel T_5 \parallel T_6$

The inverse function  $GFN_{4,r}^{-1}$  is obtained by changing the order of  $RK_i$  and the direction of word rotation at 2.2) and 3) in  $GFN_{4,r}$ .

$GFN_{4,r}^{-1}$ :

- 1)  $T_0 \parallel T_1 \parallel T_2 \parallel T_3 \leftarrow X_0 \parallel X_1 \parallel X_2 \parallel X_3$
- 2) For  $i = 0$  to  $r - 1$  do the following:
  - 2.1)  $T_1 \leftarrow T_1 \oplus F_0(RK_{2(r-i)-2}, T_0)$   
 $T_3 \leftarrow T_3 \oplus F_1(RK_{2(r-i)-1}, T_2)$
  - 2.2)  $T_0 \parallel T_1 \parallel T_2 \parallel T_3 \leftarrow T_3 \parallel T_0 \parallel T_1 \parallel T_2$
- 3)  $Y_0 \parallel Y_1 \parallel Y_2 \parallel Y_3 \leftarrow T_1 \parallel T_2 \parallel T_3 \parallel T_0$

### 6.2.5.2 F-functions

Two F-functions  $F_0$  and  $F_1$  used in  $GFN_{d,r}$  are defined as follows:

$F_0 : (RK_{(32)}, X_{(32)}) \mapsto Y_{(32)}$

- 1)  $V \leftarrow RK \oplus x$
- 2) Let  $V = V_0 \parallel V_1 \parallel V_2 \parallel V_3$ ,  $V_i \in \{0,1\}^8$ .  
 $V_0 \leftarrow S_0(V_0)$   
 $V_1 \leftarrow S_1(V_1)$

$$V_2 \leftarrow S_0(V_2)$$

$$V_3 \leftarrow S_1(V_3)$$

3) Let  $y = y_0 \parallel y_1 \parallel y_2 \parallel y_3$ ,  $y_i \in \{0,1\}^8$ .

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{pmatrix} \leftarrow M_0 \begin{pmatrix} V_0 \\ V_1 \\ V_2 \\ V_3 \end{pmatrix}$$

$$F_1 : (RK_{(32)}, x_{(32)}) \mapsto y_{(32)}$$

1)  $V \leftarrow RK \oplus x$

2) Let  $V = V_0 \parallel V_1 \parallel V_2 \parallel V_3$ ,  $V_i \in \{0,1\}^8$ .

$$V_0 \leftarrow S_1(V_0)$$

$$V_1 \leftarrow S_0(V_1)$$

$$V_2 \leftarrow S_1(V_2)$$

$$V_3 \leftarrow S_0(V_3)$$

3) Let  $y = y_0 \parallel y_1 \parallel y_2 \parallel y_3$ ,  $y_i \in \{0,1\}^8$ .

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{pmatrix} \leftarrow M_1 \begin{pmatrix} V_0 \\ V_1 \\ V_2 \\ V_3 \end{pmatrix}$$

$S_0$  and  $S_1$  are nonlinear 8-bit S-boxes described in 6.2.5.3, and  $M_0$  and  $M_1$  are  $4 \times 4$  diffusion matrices described in 6.2.5.4. In each F-function two S-boxes and a matrix are used, but the S-boxes are used in a different order and the matrices differ. Figure 7 shows a graphical representation of the F-functions.

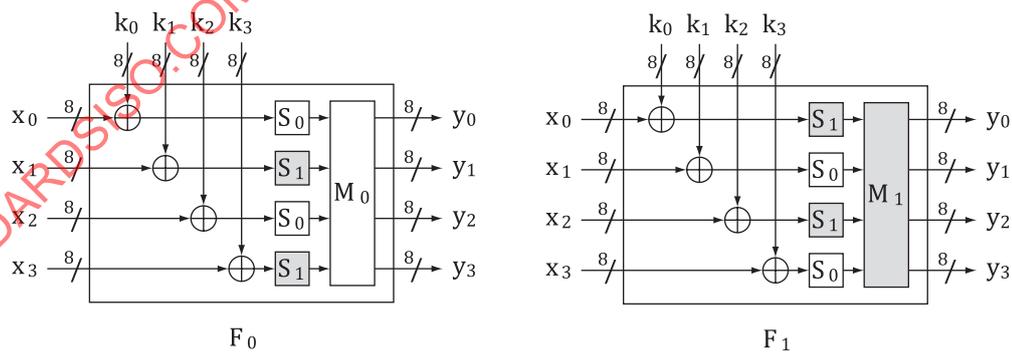


Figure 7 — F-functions

### 6.2.5.3 S-boxes

CLEFIA employs two different types of 8-bit S-boxes  $S_0$  and  $S_1$ :  $S_0$  is based on four 4-bit random S-boxes, and  $S_1$  is based on the inverse function over  $GF(2^8)$ .

Tables 5 and 6 show the output values of  $S_0$  and  $S_1$ , respectively. In these tables all values are expressed in a hexadecimal notation. For an 8-bit input of an S-box, the upper 4 bits indicate a row and the lower

4 bits indicate a column. For example, if a value  $0xab$  is input,  $0x7e$  is output by  $S_0$  because it is on the cross line of the row indexed by 'a.' and the column indexed by '.b'.

Table 5 —  $S_0$

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

Table 6 —  $S_1$

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

a) S-box  $S_0$

$S_0 : \{0,1\}^8 \rightarrow \{0,1\}^8 : x \mapsto y = S_0(x)$  is generated by combining four 4-bit S-boxes  $SS_0, SS_1, SS_2$  and  $SS_3$  in the following way. The values of these S-boxes are defined in Table 7.

- 1)  $t_0 \leftarrow SS_0(x_0), t_1 \leftarrow SS_1(x_1)$ , where  $x = x_0 \parallel x_1, x_i \in \{0,1\}^4$
- 2)  $u_0 \leftarrow t_0 \oplus_{0 \times 2} t_1, u_1 \leftarrow 0 \times 2 \cdot t_0 \oplus t_1$
- 3)  $y_0 \leftarrow SS_2(u_0), y_1 \leftarrow SS_3(u_1)$ , where  $y = y_0 \parallel y_1, y_i \in \{0,1\}^4$

The multiplication in  $_{0 \times 2}t_i$  is performed in  $GF(2^4)$  defined by the lexicographically first primitive polynomial  $z^4 + z + 1$ . Figure 8 shows the construction of  $S_0$ .

Table 7 —  $SS_i$  ( $0 \leq i < 4$ )

| x         | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e | f |
|-----------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $SS_0(x)$ | e | 6 | c | a | 8 | 7 | 2 | f | b | 1 | 4 | 0 | 5 | 9 | d | 3 |
| $SS_1(x)$ | 6 | 4 | 0 | d | 2 | b | a | 3 | 9 | c | e | f | 8 | 7 | 5 | 1 |
| $SS_2(x)$ | b | 8 | 5 | e | a | 6 | 4 | c | f | 7 | 2 | 3 | 1 | 0 | d | 9 |
| $SS_3(x)$ | a | 2 | 6 | d | 3 | 4 | 5 | e | 0 | 7 | 8 | 9 | b | f | c | 1 |

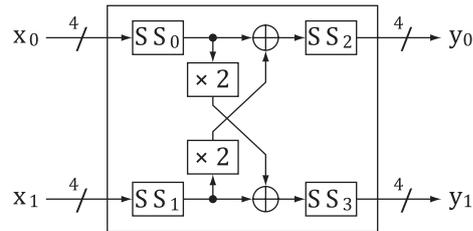


Figure 8 —  $S_0$

b) S-box  $S_1$

$S_1 : \{0,1\}^8 \rightarrow \{0,1\}^8 : x \mapsto y = S_1(x)$  is defined as follows:

$$y = \begin{cases} g((f(x))^{-1}) & \text{if } f(x) \neq 0 \\ g(0) & \text{if } f(x) = 0 \end{cases}$$

The inverse function is performed in  $GF(2^8)$  defined by a primitive polynomial  $z^8 + z^4 + z^3 + z^2 + 1$  ( $=0x11d$ ).  $f$  and  $g$  are affine transformations over  $GF(2)$ , which are defined as follows.

$$f : \{0,1\}^8 \rightarrow \{0,1\}^8 : x \mapsto y = f(x),$$

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

$$g : \{0,1\}^8 \rightarrow \{0,1\}^8 : x \mapsto y = g(x),$$

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Here,  $x = x_0 \parallel x_1 \parallel x_2 \parallel x_3 \parallel x_4 \parallel x_5 \parallel x_6 \parallel x_7$  and  $y = y_0 \parallel y_1 \parallel y_2 \parallel y_3 \parallel y_4 \parallel y_5 \parallel y_6 \parallel y_7$ ,  $x_i, y_i \in \{0,1\}$ . The constants in  $f$  and  $g$  can be represented as  $0_{x1e}$  and  $0_{x69}$ , respectively.

### 6.2.5.4 Diffusion matrices

The matrices  $M_0$  and  $M_1$  are defined as follows.

$$M_0 = \begin{pmatrix} 01 & 02 & 04 & 06 \\ 02 & 01 & 06 & 04 \\ 04 & 06 & 01 & 02 \\ 06 & 04 & 02 & 01 \end{pmatrix}, M_1 = \begin{pmatrix} 01 & 08 & 02 & 0a \\ 08 & 01 & 0a & 02 \\ 02 & 0a & 01 & 08 \\ 0a & 02 & 08 & 01 \end{pmatrix}$$

The multiplications of a matrix and a vector are performed in  $GF(2^8)$  defined by the lexicographically first primitive polynomial  $z^8 + z^4 + z^3 + z^2 + 1$  ( $=0_{x11d}$ ).

### 6.2.6 CLEFIA key schedule

#### 6.2.6.1 Overall structure

The key schedule of CLEFIA supports 128, 192 and 256-bit keys and outputs whitening keys  $WK_i$  ( $0 \leq i < 4$ ) and round keys  $RK_j$  ( $0 \leq j < 2r$ ) for the data processing part. Let  $K$  be the key and  $L$  be an intermediate key. The key schedule consists of the following two steps.

- 1) Generating  $L$  from  $K$ .
- 2) Expanding  $K$  and  $L$  (Generating  $WK_i$  and  $RK_j$ ).

To generate  $L$  from  $K$ , the key schedule for a 128-bit key uses a 128-bit permutation  $GFN_{4,12}$ , while the key schedules for 192/256-bit keys use a 256-bit permutation  $GFN_{8,10}$ .

**6.2.6.2 Key schedule for a 128-bit key**

The 128-bit intermediate key  $L$  is generated in step 1 by applying  $GFN_{4,12}$  which takes twenty-four 32-bit constant values  $CON_i^{(128)}$  ( $0 \leq i < 24$ ) as round keys and  $K = K_0 \parallel K_1 \parallel K_2 \parallel K_3$  as an input. Then  $K$  and  $L$  are used to generate  $WK_i$  ( $0 \leq i < 4$ ) and  $RK_j$  ( $0 \leq j < 36$ ) in steps 2 and 3. The thirty-six 32-bit constant values  $CON_i^{(128)}$  ( $24 \leq i < 60$ ) used in step 3 are defined in 6.2.6.6. The DoubleSwap function  $\Sigma$  is defined in 6.2.6.5.

(Generating  $L$  from  $K$ )

$$1) \quad L \leftarrow GFN_{4,12} \left( CON_0^{(128)}, \dots, CON_{23}^{(128)}, K_0, \dots, K_3 \right)$$

(Expanding  $K$  and  $L$ )

$$2) \quad WK_0 \parallel WK_1 \parallel WK_2 \parallel WK_3 \leftarrow K$$

3) For  $i = 0$  to 8, do the following:

$$T \leftarrow L \oplus \left( CON_{24+4i}^{(128)} \parallel CON_{24+4i+1}^{(128)} \parallel CON_{24+4i+2}^{(128)} \parallel CON_{24+4i+3}^{(128)} \right)$$

$$L \leftarrow \Sigma(L)$$

if  $i$  is odd:  $T \leftarrow T \oplus K$

$$RK_{4i} \parallel RK_{4i+1} \parallel RK_{4i+2} \parallel RK_{4i+3} \leftarrow T$$

Table 8 shows the relationship between generated round keys and related data.

**Table 8 — Expanding  $K$  and  $L$  (128-bit key)**

|   |  |
|---|--|
| $WK_0 \parallel WK_1 \parallel WK_2 \parallel WK_3$             | $K$  |
| $RK_0 \parallel RK_1 \parallel RK_2 \parallel RK_3$             | $L \oplus \left( CON_{24}^{(128)} \parallel CON_{25}^{(128)} \parallel CON_{26}^{(128)} \parallel CON_{27}^{(128)} \right)$                    |
| $RK_4 \parallel RK_5 \parallel RK_6 \parallel RK_7$             | $\Sigma(L) \oplus K \oplus \left( CON_{28}^{(128)} \parallel CON_{29}^{(128)} \parallel CON_{30}^{(128)} \parallel CON_{31}^{(128)} \right)$   |
| $RK_8 \parallel RK_9 \parallel RK_{10} \parallel RK_{11}$       | $\Sigma^2(L) \oplus \left( CON_{32}^{(128)} \parallel CON_{33}^{(128)} \parallel CON_{34}^{(128)} \parallel CON_{35}^{(128)} \right)$          |
| $RK_{12} \parallel RK_{13} \parallel RK_{14} \parallel RK_{15}$ | $\Sigma^3(L) \oplus K \oplus \left( CON_{36}^{(128)} \parallel CON_{37}^{(128)} \parallel CON_{38}^{(128)} \parallel CON_{39}^{(128)} \right)$ |
| $RK_{16} \parallel RK_{17} \parallel RK_{18} \parallel RK_{19}$ | $\Sigma^4(L) \oplus \left( CON_{40}^{(128)} \parallel CON_{41}^{(128)} \parallel CON_{42}^{(128)} \parallel CON_{43}^{(128)} \right)$          |
| $RK_{20} \parallel RK_{21} \parallel RK_{22} \parallel RK_{23}$ | $\Sigma^5(L) \oplus K \oplus \left( CON_{44}^{(128)} \parallel CON_{45}^{(128)} \parallel CON_{46}^{(128)} \parallel CON_{47}^{(128)} \right)$ |
| $RK_{24} \parallel RK_{25} \parallel RK_{26} \parallel RK_{27}$ | $\Sigma^6(L) \oplus \left( CON_{48}^{(128)} \parallel CON_{49}^{(128)} \parallel CON_{50}^{(128)} \parallel CON_{51}^{(128)} \right)$          |
| $RK_{28} \parallel RK_{29} \parallel RK_{30} \parallel RK_{31}$ | $\Sigma^7(L) \oplus K \oplus \left( CON_{52}^{(128)} \parallel CON_{53}^{(128)} \parallel CON_{54}^{(128)} \parallel CON_{55}^{(128)} \right)$ |
| $RK_{32} \parallel RK_{33} \parallel RK_{34} \parallel RK_{35}$ | $\Sigma^8(L) \oplus \left( CON_{56}^{(128)} \parallel CON_{57}^{(128)} \parallel CON_{58}^{(128)} \parallel CON_{59}^{(128)} \right)$          |

**6.2.6.3 Key schedule for a 192-bit key**

Two 128-bit values  $K_L$  and  $K_R$  are generated from a 192-bit key  $K = K_0 \parallel K_1 \parallel K_2 \parallel K_3 \parallel K_4 \parallel K_5$ , where  $K_i \in \{0,1\}^{32}$ . Then two 128-bit values  $L_L$  and  $L_R$  are generated by applying  $GFN_{8,10}$  which takes  $CON_i^{(192)}$  ( $0 \leq i < 40$ ) as round keys and  $K_L \parallel K_R$  as a 256-bit input. Figure 9 shows the construction of  $GFN_{8,10}$ .

$K_L, K_R$  and  $L_L, L_R$  are used to generate  $WK_i$  ( $0 \leq i < 4$ ) and  $RK_j$  ( $0 \leq j < 44$ ) in steps 4 and 5 below. In the latter part, forty-four 32-bit constant values  $CON_i^{(192)}$  ( $40 \leq i < 84$ ) are used.

The following steps show the 192-bit/256-bit key schedule. For the 192-bit key schedule, the value of  $k$  is set as 192.

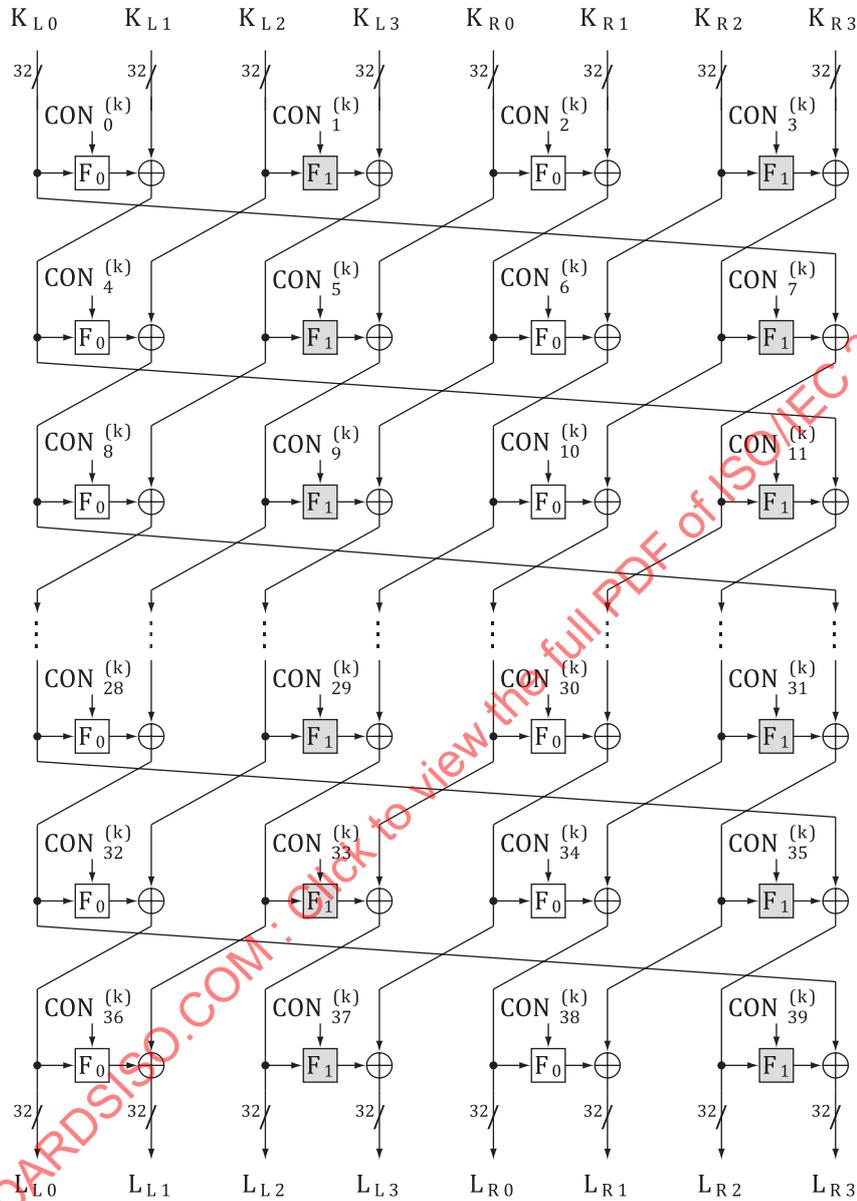


Figure 9 — Structure of  $GFN_{8,10}$

(Generating  $L_L, L_R$  from  $K_L, K_R$  for a  $k$ -bit key)

- 1) Set  $k = 192$  or  $k = 256$
- 2) If  $k = 192$  :  $K_L \leftarrow K_0 \parallel K_1 \parallel K_2 \parallel K_3, K_R \leftarrow K_4 \parallel K_5 \parallel \sim K_0 \parallel \sim K_1$   
 else if  $k = 256$  :  $K_L \leftarrow K_0 \parallel K_1 \parallel K_2 \parallel K_3, K_R \leftarrow K_4 \parallel K_5 \parallel K_6 \parallel K_7$
- 3) Let  $K_L = K_{L0} \parallel K_{L1} \parallel K_{L2} \parallel K_{L3}, K_R = K_{R0} \parallel K_{R1} \parallel K_{R2} \parallel K_{R3}$

$$L_L \parallel L_R \leftarrow GFN_{8,10} \left( CON_0^{(k)}, \dots, CON_{39}^{(k)}, K_{L0}, \dots, K_{L3}, K_{R0}, \dots, K_{R3} \right)$$

(Expanding  $K_L, K_R$  and  $L_L, L_R$  for a  $k$ -bit key)

4)  $WK_0 \parallel WK_1 \parallel WK_2 \parallel WK_3 \leftarrow K_L \oplus K_R$

5) For  $i = 0$  to 10 (if  $k = 192$ ), or 12 (if  $k = 256$ ) do the following:

If  $(i \bmod 4) = 0$  or 1:

$$T \leftarrow L_L \oplus \left( CON_{40+4i}^{(k)} \parallel CON_{40+4i+1}^{(k)} \parallel CON_{40+4i+2}^{(k)} \parallel CON_{40+4i+3}^{(k)} \right)$$

$$L_L \leftarrow \Sigma(L_L)$$

if  $i$  is odd:  $T \leftarrow T \oplus K_R$

else:

$$T \leftarrow L_R \oplus \left( CON_{40+4i}^{(k)} \parallel CON_{40+4i+1}^{(k)} \parallel CON_{40+4i+2}^{(k)} \parallel CON_{40+4i+3}^{(k)} \right)$$

$$L_R \leftarrow \Sigma(L_R)$$

if  $i$  is odd:  $T \leftarrow T \oplus K_L$

$$RK_{4i} \parallel RK_{4i+1} \parallel RK_{4i+2} \parallel RK_{4i+3} \leftarrow T$$

Table 9 shows the relationship between generated round keys and related data.

**Table 9 — Expanding  $K_L, K_R, L_L$  and  $L_R$  (192-bit key)**

|   |  |
|---|--|
| $WK_0 \parallel WK_1 \parallel WK_2 \parallel WK_3$             | $K_L \oplus K_R$   |
| $RK_0 \parallel RK_1 \parallel RK_2 \parallel RK_3$             | $L_L \oplus \left( CON_{40}^{(192)} \parallel CON_{41}^{(192)} \parallel CON_{42}^{(192)} \parallel CON_{43}^{(192)} \right)$                      |
| $RK_4 \parallel RK_5 \parallel RK_6 \parallel RK_7$             | $\Sigma(L_L) \oplus K_R \oplus \left( CON_{44}^{(192)} \parallel CON_{45}^{(192)} \parallel CON_{46}^{(192)} \parallel CON_{47}^{(192)} \right)$   |
| $RK_8 \parallel RK_9 \parallel RK_{10} \parallel RK_{11}$       | $L_R \oplus \left( CON_{48}^{(192)} \parallel CON_{49}^{(192)} \parallel CON_{50}^{(192)} \parallel CON_{51}^{(192)} \right)$                      |
| $RK_{12} \parallel RK_{13} \parallel RK_{14} \parallel RK_{15}$ | $\Sigma(L_R) \oplus K_L \oplus \left( CON_{52}^{(192)} \parallel CON_{53}^{(192)} \parallel CON_{54}^{(192)} \parallel CON_{55}^{(192)} \right)$   |
| $RK_{16} \parallel RK_{17} \parallel RK_{18} \parallel RK_{19}$ | $\Sigma^2(L_L) \oplus \left( CON_{56}^{(192)} \parallel CON_{57}^{(192)} \parallel CON_{58}^{(192)} \parallel CON_{59}^{(192)} \right)$            |
| $RK_{20} \parallel RK_{21} \parallel RK_{22} \parallel RK_{23}$ | $\Sigma^3(L_L) \oplus K_R \oplus \left( CON_{60}^{(192)} \parallel CON_{61}^{(192)} \parallel CON_{62}^{(192)} \parallel CON_{63}^{(192)} \right)$ |
| $RK_{24} \parallel RK_{25} \parallel RK_{26} \parallel RK_{27}$ | $\Sigma^2(L_R) \oplus \left( CON_{64}^{(192)} \parallel CON_{65}^{(192)} \parallel CON_{66}^{(192)} \parallel CON_{67}^{(192)} \right)$            |
| $RK_{28} \parallel RK_{29} \parallel RK_{30} \parallel RK_{31}$ | $\Sigma^3(L_R) \oplus K_L \oplus \left( CON_{68}^{(192)} \parallel CON_{69}^{(192)} \parallel CON_{70}^{(192)} \parallel CON_{71}^{(192)} \right)$ |
| $RK_{32} \parallel RK_{33} \parallel RK_{34} \parallel RK_{35}$ | $\Sigma^4(L_L) \oplus \left( CON_{72}^{(192)} \parallel CON_{73}^{(192)} \parallel CON_{74}^{(192)} \parallel CON_{75}^{(192)} \right)$            |
| $RK_{36} \parallel RK_{37} \parallel RK_{38} \parallel RK_{39}$ | $\Sigma^5(L_L) \oplus K_R \oplus \left( CON_{76}^{(192)} \parallel CON_{77}^{(192)} \parallel CON_{78}^{(192)} \parallel CON_{79}^{(192)} \right)$ |
| $RK_{40} \parallel RK_{41} \parallel RK_{42} \parallel RK_{43}$ | $\Sigma^4(L_R) \oplus \left( CON_{80}^{(192)} \parallel CON_{81}^{(192)} \parallel CON_{82}^{(192)} \parallel CON_{83}^{(192)} \right)$            |

#### 6.2.6.4 Key schedule for a 256-bit key

The key schedule for a 256-bit key is almost the same as that for 192-bit key, except for constant values, the required number of  $RK_i$ , and the initialization of  $K_R$ .

For a 256-bit key, the value of  $k$  is set as 256, and the steps are almost the same as in the 192-bit key case (see description in 6.2.6.3). The difference is that the first forty 32-bit constant values,  $CON_i^{(256)}$  ( $0 \leq i < 40$ ), are used as round keys to generate  $L_L$  and  $L_R$ , and the last fifty-two 32-bit constant values,  $CON_i^{(256)}$  ( $40 \leq i < 92$ ), are used to generate  $RK_j$  ( $0 \leq j < 52$ ).

Table 10 shows the relationship between generated round keys and related data.

**Table 10 — Expanding  $K_L, K_R, L_L$  and  $L_R$  (256-bit key)**

|                                   |   |
|-----------------------------------|---|
| $WK_0 WK_1 WK_2 WK_3$             | $K_L \oplus K_R$  |
| $RK_0 RK_1 RK_2 RK_3$             | $L_L \oplus (CON_{40}^{(256)} \parallel CON_{41}^{(256)} \parallel CON_{42}^{(256)} \parallel CON_{43}^{(256)})$                      |
| $RK_4 RK_5 RK_6 RK_7$             | $\Sigma(L_L) \oplus K_R \oplus (CON_{44}^{(256)} \parallel CON_{45}^{(256)} \parallel CON_{46}^{(256)} \parallel CON_{47}^{(256)})$   |
| $RK_8 RK_9 RK_{10} RK_{11}$       | $L_R \oplus (CON_{48}^{(256)} \parallel CON_{49}^{(256)} \parallel CON_{50}^{(256)} \parallel CON_{51}^{(256)})$                      |
| $RK_{12} RK_{13} RK_{14} RK_{15}$ | $\Sigma(L_R) \oplus K_L \oplus (CON_{52}^{(256)} \parallel CON_{53}^{(256)} \parallel CON_{54}^{(256)} \parallel CON_{55}^{(256)})$   |
| $RK_{16} RK_{17} RK_{18} RK_{19}$ | $\Sigma^2(L_L) \oplus (CON_{56}^{(256)} \parallel CON_{57}^{(256)} \parallel CON_{58}^{(256)} \parallel CON_{59}^{(256)})$            |
| $RK_{20} RK_{21} RK_{22} RK_{23}$ | $\Sigma^3(L_L) \oplus K_R \oplus (CON_{60}^{(256)} \parallel CON_{61}^{(256)} \parallel CON_{62}^{(256)} \parallel CON_{63}^{(256)})$ |
| $RK_{24} RK_{25} RK_{26} RK_{27}$ | $\Sigma^2(L_R) \oplus (CON_{64}^{(256)} \parallel CON_{65}^{(256)} \parallel CON_{66}^{(256)} \parallel CON_{67}^{(256)})$            |
| $RK_{28} RK_{29} RK_{30} RK_{31}$ | $\Sigma^3(L_R) \oplus K_L \oplus (CON_{68}^{(256)} \parallel CON_{69}^{(256)} \parallel CON_{70}^{(256)} \parallel CON_{71}^{(256)})$ |
| $RK_{32} RK_{33} RK_{34} RK_{35}$ | $\Sigma^4(L_L) \oplus (CON_{72}^{(256)} \parallel CON_{73}^{(256)} \parallel CON_{74}^{(256)} \parallel CON_{75}^{(256)})$            |
| $RK_{36} RK_{37} RK_{38} RK_{39}$ | $\Sigma^5(L_L) \oplus K_R \oplus (CON_{76}^{(256)} \parallel CON_{77}^{(256)} \parallel CON_{78}^{(256)} \parallel CON_{79}^{(256)})$ |
| $RK_{40} RK_{41} RK_{42} RK_{43}$ | $\Sigma^4(L_R) \oplus (CON_{80}^{(256)} \parallel CON_{81}^{(256)} \parallel CON_{82}^{(256)} \parallel CON_{83}^{(256)})$            |
| $RK_{44} RK_{45} RK_{46} RK_{47}$ | $\Sigma^5(L_R) \oplus K_L \oplus (CON_{84}^{(256)} \parallel CON_{85}^{(256)} \parallel CON_{86}^{(256)} \parallel CON_{87}^{(256)})$ |
| $RK_{48} RK_{49} RK_{50} RK_{51}$ | $\Sigma^6(L_L) \oplus (CON_{88}^{(256)} \parallel CON_{89}^{(256)} \parallel CON_{90}^{(256)} \parallel CON_{91}^{(256)})$            |

**6.2.6.5 DoubleSwap function**

The DoubleSwap function  $\Sigma: \{0,1\}^{128} \rightarrow \{0,1\}^{128}$  is defined as follows:

$$X_{(128)} \mapsto Y_{(128)}$$

$$Y = X[7-63] \parallel X[121-127] \parallel X[0-6] \parallel X[64-120],$$

where  $X[a-b]$  denotes a bit string cut from the  $a$ -th bit to the  $b$ -th bit of  $X$ . Bit 0 is the most significant bit.

The DoubleSwap function is illustrated in Figure 10.



**Table 12 (continued)**

|               |      |      |      |      |      |      |      |      |
|---------------|------|------|------|------|------|------|------|------|
| <i>i</i>      | 16   | 17   | 18   | 19   | 20   | 21   | 22   | 23   |
| $T_i^{(128)}$ | 87aa | 43d5 | f5f2 | 7af9 | e964 | 74b2 | 3a59 | c934 |
| <i>i</i>      | 24   | 25   | 26   | 27   | 28   | 29   |      |      |
| $T_i^{(128)}$ | 649a | 324d | cd3e | 669f | e757 | a7b3 |      |      |

**Table 13 —  $T_i^{(192)}$**

|               |      |      |      |      |      |      |      |      |
|---------------|------|------|------|------|------|------|------|------|
| <i>i</i>      | 0    | 1    | 2    | 3    | 4    | 5    | 6    | 7    |
| $T_i^{(192)}$ | 7137 | ec83 | a259 | 8534 | 429a | 214d | c4be | 625f |
| <i>i</i>      | 8    | 9    | 10   | 11   | 12   | 13   | 14   | 15   |
| $T_i^{(192)}$ | e537 | a683 | 8759 | 97b4 | 4bda | 25ed | c6ee | 6377 |
| <i>i</i>      | 16   | 17   | 18   | 19   | 20   | 21   | 22   | 23   |
| $T_i^{(192)}$ | e5a3 | a6c9 | 877c | 43be | 21df | c4f7 | b663 | 8f29 |
| <i>i</i>      | 24   | 25   | 26   | 27   | 28   | 29   | 30   | 31   |
| $T_i^{(192)}$ | 938c | 49c6 | 24e3 | c669 | b72c | 5b96 | 2dcb | c2fd |
| <i>i</i>      | 32   | 33   | 34   | 35   | 36   | 37   | 38   | 39   |
| $T_i^{(192)}$ | b566 | 5ab3 | f941 | a8b8 | 545c | 2a2e | 1517 | de93 |
| <i>i</i>      | 40   | 41   |      |      |      |      |      |      |
| $T_i^{(192)}$ | bb51 | 89b0 |      |      |      |      |      |      |

**Table 14 —  $T_i^{(256)}$**

|               |      |      |      |      |      |      |      |      |
|---------------|------|------|------|------|------|------|------|------|
| <i>i</i>      | 0    | 1    | 2    | 3    | 4    | 5    | 6    | 7    |
| $T_i^{(256)}$ | b5c0 | 5ae0 | 2d70 | 16b8 | 0b5c | 05ae | 02d7 | d573 |
| <i>i</i>      | 8    | 9    | 10   | 11   | 12   | 13   | 14   | 15   |
| $T_i^{(256)}$ | bea1 | 8b48 | 45a4 | 22d2 | 1169 | dcac | 6e56 | 372b |
| <i>i</i>      | 16   | 17   | 18   | 19   | 20   | 21   | 22   | 23   |
| $T_i^{(256)}$ | ef8d | b3de | 59ef | f8ef | a86f | 802f | 940f | 9e1f |
| <i>i</i>      | 24   | 25   | 26   | 27   | 28   | 29   | 30   | 31   |
| $T_i^{(256)}$ | 9b17 | 9993 | 98d1 | 9870 | 4c38 | 261c | 130e | 0987 |
| <i>i</i>      | 32   | 33   | 34   | 35   | 36   | 37   | 38   | 39   |
| $T_i^{(256)}$ | d0db | bc75 | 8a22 | 4511 | f690 | 7b48 | 3da4 | 1ed2 |
| <i>i</i>      | 40   | 41   | 42   | 43   | 44   | 45   |      |      |
| $T_i^{(256)}$ | 0f69 | d3ac | 69d6 | 34eb | ce6d | b32e |      |      |

**Table 15 —  $CON_i^{(128)}$**

|                 |          |          |          |          |
|-----------------|----------|----------|----------|----------|
| <i>i</i>        | 0        | 1        | 2        | 3        |
| $CON_i^{(128)}$ | f56b7aeb | 994a8a42 | 96a4bd75 | fa854521 |
| <i>i</i>        | 4        | 5        | 6        | 7        |

Table 15 (continued)

|                 |          |          |          |          |
|-----------------|----------|----------|----------|----------|
| $CON_i^{(128)}$ | 735b768a | 1f7abac4 | d5bc3b45 | b99d5d62 |
| $i$             | 8        | 9        | 10       | 11       |
| $CON_i^{(128)}$ | 52d73592 | 3ef636e5 | c57a1ac9 | a95b9b72 |
| $i$             | 12       | 13       | 14       | 15       |
| $CON_i^{(128)}$ | 5ab42554 | 369555ed | 1553ba9a | 7972b2a2 |
| $i$             | 16       | 17       | 18       | 19       |
| $CON_i^{(128)}$ | e6b85d4d | 8a995951 | 4b550696 | 2774b4fc |
| $i$             | 20       | 21       | 22       | 23       |
| $CON_i^{(128)}$ | c9bb034b | a59a5a7e | 88cc81a5 | e4ed2d3f |
| $i$             | 24       | 25       | 26       | 27       |
| $CON_i^{(128)}$ | 7c6f68e2 | 104e8ecb | d2263471 | be01c765 |
| $i$             | 28       | 29       | 30       | 31       |
| $CON_i^{(128)}$ | 511a3208 | 3d3bfbe6 | 1084b134 | 7ca565a7 |
| $i$             | 32       | 33       | 34       | 35       |
| $CON_i^{(128)}$ | 304bf0aa | 5c6aaa87 | f4347855 | 9815d543 |
| $i$             | 36       | 37       | 38       | 39       |
| $CON_i^{(128)}$ | 4213141a | 2e32f2f5 | cd180a0d | a139f97a |
| $i$             | 40       | 41       | 42       | 43       |
| $CON_i^{(128)}$ | 5e852d36 | 32a464e9 | c353169b | af72b274 |
| $i$             | 44       | 45       | 46       | 47       |
| $CON_i^{(128)}$ | 8db89b4d | e199593a | 7ed56d96 | 12f434c9 |
| $i$             | 48       | 49       | 50       | 51       |
| $CON_i^{(128)}$ | d37b36cb | bf5a9a64 | 85ac9b65 | e98d4d32 |
| $i$             | 52       | 53       | 54       | 55       |
| $CON_i^{(128)}$ | 7adf6582 | 16fe3ecd | d17e32c1 | bd5f9f66 |
| $i$             | 56       | 57       | 58       | 59       |
| $CON_i^{(128)}$ | 50b63150 | 3c9757e7 | 1052b098 | 7c73b3a7 |

Table 16 —  $CON_i^{(192)}$ 

|                 |          |          |          |          |
|-----------------|----------|----------|----------|----------|
| $i$             | 0        | 1        | 2        | 3        |
| $CON_i^{(192)}$ | c6d61d91 | aa7f3771 | 5b6226f8 | 374383ec |
| $i$             | 4        | 5        | 6        | 7        |
| $CON_i^{(192)}$ | 15b8bb4c | 799959a2 | 32d5f596 | 5ef43485 |
| $i$             | 8        | 9        | 10       | 11       |
| $CON_i^{(192)}$ | f57b7acb | 995a9a42 | 96acbd65 | fa8d4d21 |
| $i$             | 12       | 13       | 14       | 15       |
| $CON_i^{(192)}$ | 735f7682 | 1f7ebec4 | d5be3b41 | b99f5f62 |

Table 16 (continued)

|                 |          |          |          |          |
|-----------------|----------|----------|----------|----------|
| <i>i</i>        | 16       | 17       | 18       | 19       |
| $CON_i^{(192)}$ | 52d63590 | 3ef737e5 | 1162b2f8 | 7d4383a6 |
| <i>i</i>        | 20       | 21       | 22       | 23       |
| $CON_i^{(192)}$ | 30b8f14c | 5c995987 | 2055d096 | 4c74b497 |
| <i>i</i>        | 24       | 25       | 26       | 27       |
| $CON_i^{(192)}$ | fc3b684b | 901ada4b | 920cb425 | fe2ded25 |
| <i>i</i>        | 28       | 29       | 30       | 31       |
| $CON_i^{(192)}$ | 710f7222 | 1d2eeec6 | d4963911 | b8b77763 |
| <i>i</i>        | 32       | 33       | 34       | 35       |
| $CON_i^{(192)}$ | 524234b8 | 3e63a3e5 | 1128b26c | 7d09e9a6 |
| <i>i</i>        | 36       | 37       | 38       | 39       |
| $CON_i^{(192)}$ | 309df106 | 5cbc7c87 | f45f7883 | 987ebe43 |
| <i>i</i>        | 40       | 41       | 42       | 43       |
| $CON_i^{(192)}$ | 963ebc41 | fa1fdf21 | 73167610 | 1f37f7c4 |
| <i>i</i>        | 44       | 45       | 46       | 47       |
| $CON_i^{(192)}$ | 01829338 | 6da363b6 | 38c8e1ac | 54e9298f |
| <i>i</i>        | 48       | 49       | 50       | 51       |
| $CON_i^{(192)}$ | 246dd8e6 | 484c8c93 | fe276c73 | 9206c649 |
| <i>i</i>        | 52       | 53       | 54       | 55       |
| $CON_i^{(192)}$ | 9302b639 | ff23e324 | 7188732c | 1da969c6 |
| <i>i</i>        | 56       | 57       | 58       | 59       |
| $CON_i^{(192)}$ | 00cd91a6 | 6cec2cb7 | ec7748d3 | 8056965b |
| <i>i</i>        | 60       | 61       | 62       | 63       |
| $CON_i^{(192)}$ | 9a2aa469 | f60bcb2d | 751c7a04 | 193dfdc2 |
| <i>i</i>        | 64       | 65       | 66       | 67       |
| $CON_i^{(192)}$ | 02879532 | 6ea666b5 | ed524a99 | 8173b35a |
| <i>i</i>        | 68       | 69       | 70       | 71       |
| $CON_i^{(192)}$ | 4ea00d7c | 228141f9 | 1f59ae8e | 7378b8a8 |
| <i>i</i>        | 72       | 73       | 74       | 75       |
| $CON_i^{(192)}$ | e3bd5747 | 8f9c5c54 | 9dcfaba3 | f1ee2e2a |
| <i>i</i>        | 76       | 77       | 78       | 79       |
| $CON_i^{(192)}$ | a2f6d5d1 | ced71715 | 697242d8 | 055393de |
| <i>i</i>        | 80       | 81       | 82       | 83       |
| $CON_i^{(192)}$ | 0cb0895c | 609151bb | 3e51ec9e | 5270b089 |

Table 17 —  $CON_i^{(256)}$ 

|                 |          |          |          |          |
|-----------------|----------|----------|----------|----------|
| $i$             | 0        | 1        | 2        | 3        |
| $CON_i^{(256)}$ | 0221947e | 6e00c0b5 | ed014a3f | 8120e05a |
| $i$             | 4        | 5        | 6        | 7        |
| $CON_i^{(256)}$ | 9a91a51f | f6b0702d | a159d28f | cd78b816 |
| $i$             | 8        | 9        | 10       | 11       |
| $CON_i^{(256)}$ | bcbde947 | d09c5c0b | b24ff4a3 | de6eae05 |
| $i$             | 12       | 13       | 14       | 15       |
| $CON_i^{(256)}$ | b536fa51 | d917d702 | 62925518 | 0eb373d5 |
| $i$             | 16       | 17       | 18       | 19       |
| $CON_i^{(256)}$ | 094082bc | 6561a1be | 3ca9e96e | 5088488b |
| $i$             | 20       | 21       | 22       | 23       |
| $CON_i^{(256)}$ | f24574b7 | 9e64a445 | 9533ba5b | f912d222 |
| $i$             | 24       | 25       | 26       | 27       |
| $CON_i^{(256)}$ | a688dd2d | caa96911 | 6b4d46a6 | 076cacdc |
| $i$             | 28       | 29       | 30       | 31       |
| $CON_i^{(256)}$ | d9b72353 | b596566e | 80ca91a9 | eceb2b37 |
| $i$             | 32       | 33       | 34       | 35       |
| $CON_i^{(256)}$ | 786c60e4 | 144d8dcf | 043f9842 | 681edeb3 |
| $i$             | 36       | 37       | 38       | 39       |
| $CON_i^{(256)}$ | ee0e4c21 | 822fef59 | 4f0e0e20 | 232feff8 |
| $i$             | 40       | 41       | 42       | 43       |
| $CON_i^{(256)}$ | 1f8eaf20 | 73af6fa8 | 37ceffa0 | 5bef2f80 |
| $i$             | 44       | 45       | 46       | 47       |
| $CON_i^{(256)}$ | 23eed7e0 | 4fcf0f94 | 29fec3c0 | 45df1f9e |
| $i$             | 48       | 49       | 50       | 51       |
| $CON_i^{(256)}$ | 2cf6c9d0 | 40d7179b | 2e72ccd8 | 42539399 |
| $i$             | 52       | 53       | 54       | 55       |
| $CON_i^{(256)}$ | 2f30ce5c | 4311d198 | 2f91cf1e | 43b07098 |
| $i$             | 56       | 57       | 58       | 59       |
| $CON_i^{(256)}$ | fb9678f  | 97f8384c | 91fdb3c7 | fddc1c26 |
| $i$             | 60       | 61       | 62       | 63       |
| $CON_i^{(256)}$ | a4efd9e3 | c8ce0e13 | be66ecf1 | d2478709 |
| $i$             | 64       | 65       | 66       | 67       |
| $CON_i^{(256)}$ | 673a5e48 | 0b1bdbd0 | 0b948714 | 67b575bc |
| $i$             | 68       | 69       | 70       | 71       |

Table 17 (continued)

|                 |          |          |          |          |
|-----------------|----------|----------|----------|----------|
| $CON_i^{(256)}$ | 3dc3ebba | 51e2228a | f2f075dd | 9ed11145 |
| $i$             | 72       | 73       | 74       | 75       |
| $CON_i^{(256)}$ | 417112de | 2d5090f6 | cca9096f | a088487b |
| $i$             | 76       | 77       | 78       | 79       |
| $CON_i^{(256)}$ | 8a4584b7 | e664a43d | a933c25b | c512d21e |
| $i$             | 80       | 81       | 82       | 83       |
| $CON_i^{(256)}$ | b888e12d | d4a9690f | 644d58a6 | 086cacd3 |
| $i$             | 84       | 85       | 86       | 87       |
| $CON_i^{(256)}$ | de372c53 | b216d669 | 830a9629 | ef2beb34 |
| $i$             | 88       | 89       | 90       | 91       |
| $CON_i^{(256)}$ | 798c6324 | 15ad6dce | 04cf99a2 | 68ee2eb3 |

### 6.3 LEA

#### 6.3.1 LEA algorithm

The LEA algorithm is a symmetric block cipher that processes data blocks of 128 bits and has three different key lengths: 128, 192, and 256 bits [11]. LEA with a 128-bit key, LEA with a 192-bit key, and LEA with a 256-bit key are referred to as “LEA-128”, “LEA-192” and “LEA-256”, respectively. The number of rounds is 24 for LEA-128, 28 for LEA-192, and 32 for LEA-256. The LEA encryption and decryption functions require 24, 28, or 32 round keys for LEA-128, LEA-192, or LEA-256, respectively.

#### 6.3.2 LEA specific notation

|             |   |
|-------------|---|
| $Nr$        | the number of rounds for the LEA algorithm, which is 24, 28, or 32 for the choices of key length 128, 192, or 256 bits, respectively                |
| $K_i$       | $i^{\text{th}}$ 192-bit round key consisting of six 32-bit words $K_i[0]    K_i[1]    K_i[2]    K_i[3]    K_i[4]    K_i[5]$ , where $0 \leq i < Nr$ |
| $X_i$       | $i^{\text{th}}$ 128-bit state consisting of four 32-bit words $X_i[0]    X_i[1]    X_i[2]    X_i[3]$ , where $0 \leq i \leq Nr$                     |
| $\delta[i]$ | 32-bit constant values that are used to generate round keys, where $0 \leq i < 8$   |
| $\{0,1\}^n$ | a set of $n$ -bit binary strings  |
| $\lll i$    | $i$ -bit left cyclic shift operation  |
| $\ggg i$    | $i$ -bit right cyclic shift operation   |
| $\boxplus$  | addition modulo $2^n$   |
| $\boxminus$ | subtraction modulo $2^n$  |

#### 6.3.3 LEA encryption

Let  $P = P[0] || P[1] || P[2] || P[3]$  be a 128-bit block of plaintext and  $C = C[0] || C[1] || C[2] || C[3]$  be a 128-bit block of ciphertext, where  $P[i], C[i] \in \{0,1\}^{32}$  ( $0 \leq i < 4$ ). Let  $K_i = K_i[0] || K_i[1] || K_i[2] || K_i[3] ||$

$K_i[4] \parallel K_i[5]$  ( $0 \leq i < Nr$ ) be 192-bit round keys provided by the key schedule in 6.3.5, where  $K_i[j] \in \{0,1\}^{32}$  ( $0 \leq j < 6$ ).

The encryption operation is described as follows:

(1)  $X_0[0] \parallel X_0[1] \parallel X_0[2] \parallel X_0[3] \leftarrow P[0] \parallel P[1] \parallel P[2] \parallel P[3]$

(2) for  $i = 0$  to  $(Nr - 1)$ :

$$X_{i+1}[0] \leftarrow ((X_i[0] \oplus K_i[0]) \boxplus (X_i[1] \oplus K_i[1])) \lll 9$$

$$X_{i+1}[1] \leftarrow ((X_i[1] \oplus K_i[2]) \boxplus (X_i[2] \oplus K_i[3])) \ggg 5$$

$$X_{i+1}[2] \leftarrow ((X_i[2] \oplus K_i[4]) \boxplus (X_i[3] \oplus K_i[5])) \ggg 3$$

$$X_{i+1}[3] \leftarrow X_i[0]$$

(3)  $C[0] \parallel C[1] \parallel C[2] \parallel C[3] \leftarrow X_{Nr}[0] \parallel X_{Nr}[1] \parallel X_{Nr}[2] \parallel X_{Nr}[3]$

Figure 11 shows the LEA encryption round function.

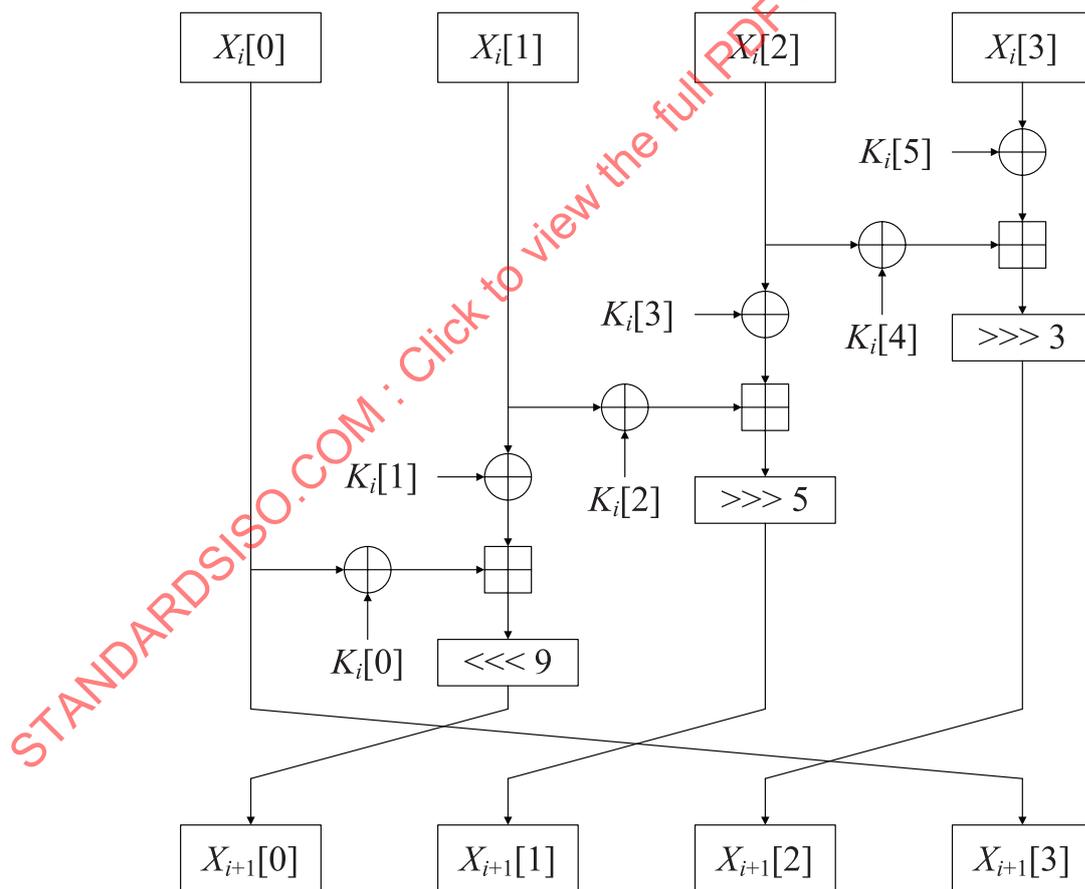


Figure 11 — LEA encryption round function

6.3.4 LEA decryption

The decryption operation is as follows:

$$(1) X_{Nr}[0] \parallel X_{Nr}[1] \parallel X_{Nr}[2] \parallel X_{Nr}[3] \leftarrow C[0] \parallel C[1] \parallel C[2] \parallel C[3]$$

(2) for  $i = (Nr - 1)$  down to 0:

$$X_i[0] \leftarrow X_{i+1}[3]$$

$$X_i[1] \leftarrow ((X_{i+1}[0] \ggg 9) \ominus (X_i[0] \oplus K_i[0])) \oplus K_i[1]$$

$$X_i[2] \leftarrow ((X_{i+1}[1] \lll 5) \ominus (X_i[1] \oplus K_i[2])) \oplus K_i[3]$$

$$X_i[3] \leftarrow ((X_{i+1}[2] \lll 3) \ominus (X_i[2] \oplus K_i[4])) \oplus K_i[5]$$

$$(3) P[0] \parallel P[1] \parallel P[2] \parallel P[3] \leftarrow X_0[0] \parallel X_0[1] \parallel X_0[2] \parallel X_0[3]$$

Figure 12 shows the LEA decryption round function.

NOTE The subtraction function in Figure 12 means that the left argument is subtracted from the top argument.

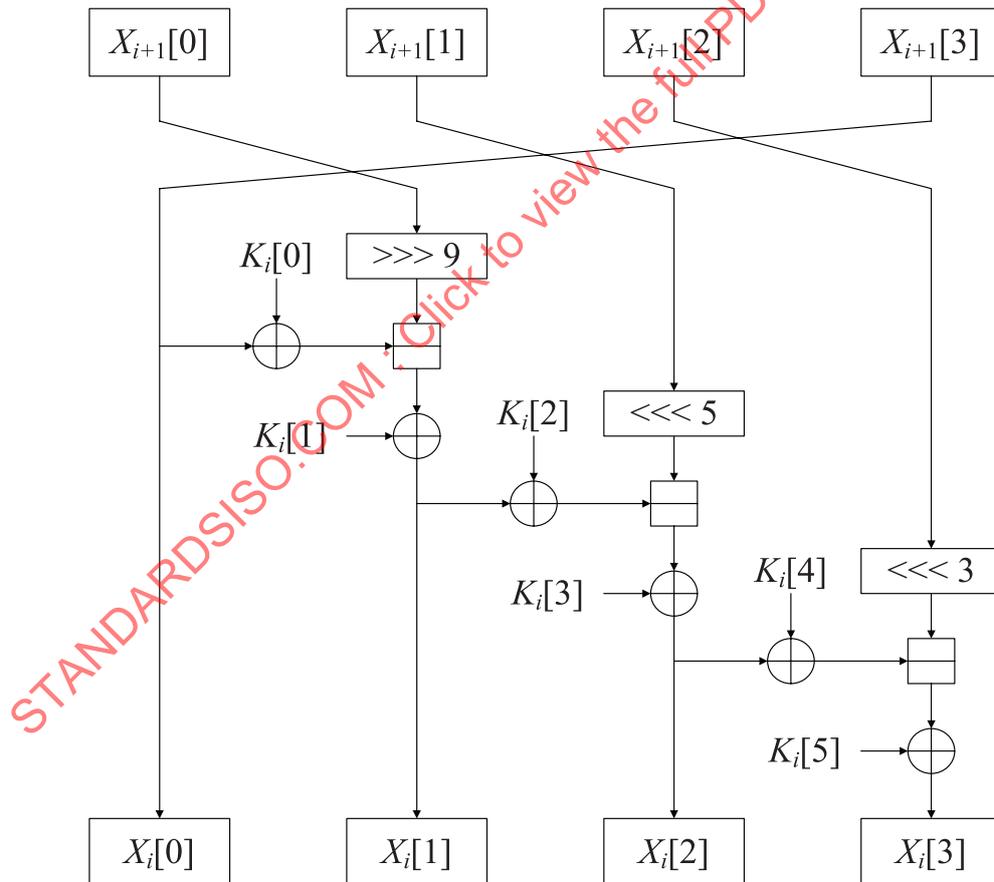


Figure 12 — LEA decryption round function

### 6.3.5 LEA key schedule

#### 6.3.5.1 Overall structure

The key schedule of LEA supports 128, 192, and 256-bit keys and outputs 192-bit round keys  $K_i$  ( $0 \leq i < Nr$ ) for the data processing part.

#### 6.3.5.2 Key schedule for LEA-128

Let  $K = K[0] \parallel K[1] \parallel K[2] \parallel K[3]$  be a 128-bit key, where  $K[i] \in \{0,1\}^{32}$  ( $0 \leq i < 4$ ). The key schedule for LEA-128 takes  $K$  and the four 32-bit constant values  $\delta[i]$  ( $0 \leq i < 4$ ) described in 6.3.5.5 as inputs and outputs twenty-four 192-bit round keys  $K_i$  ( $0 \leq i < 24$ ).

The key schedule operation for LEA-128 is as follows:

$$(1) \quad T[0] \parallel T[1] \parallel T[2] \parallel T[3] \leftarrow K[0] \parallel K[1] \parallel K[2] \parallel K[3]$$

(2) for  $i = 0$  to 23:

$$T[0] \leftarrow (T[0] \boxplus (\delta[i \bmod 4] \lll i)) \lll 1$$

$$T[1] \leftarrow (T[1] \boxplus (\delta[i \bmod 4] \lll (i+1))) \lll 3$$

$$T[2] \leftarrow (T[2] \boxplus (\delta[i \bmod 4] \lll (i+2))) \lll 6$$

$$T[3] \leftarrow (T[3] \boxplus (\delta[i \bmod 4] \lll (i+3))) \lll 11$$

$$K_i \leftarrow T[0] \parallel T[1] \parallel T[2] \parallel T[1] \parallel T[3] \parallel T[1]$$

The key schedule procedure for LEA-128 is illustrated in Figure 13.

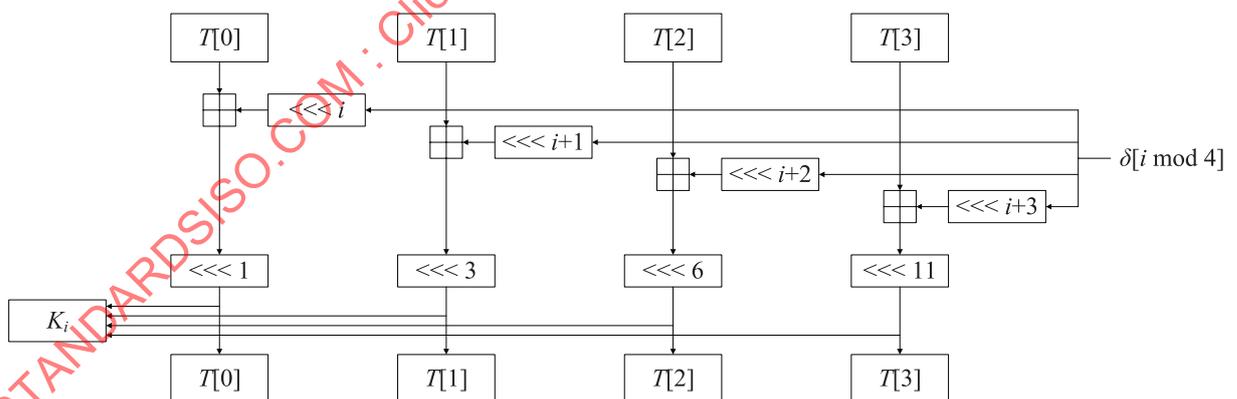


Figure 13 — The key schedule procedure for LEA-128

#### 6.3.5.3 Key schedule for LEA-192

Let  $K = K[0] \parallel K[1] \parallel K[2] \parallel K[3] \parallel K[4] \parallel K[5]$  be a 192-bit key, where  $K[i] \in \{0,1\}^{32}$  ( $0 \leq i < 6$ ). The key schedule for LEA-192 takes  $K$  and the six 32-bit constant values  $\delta[i]$  ( $0 \leq i < 6$ ) described in 6.3.5.5 as inputs and outputs twenty-eight 192-bit round keys  $K_i$  ( $0 \leq i < 28$ ).

The key schedule operation for LEA-192 is as follows:

- (1)  $T[0]||T[1]||T[2]||T[3]||T[4]||T[5] \leftarrow K[0]||K[1]||K[2]||K[3]||K[4]||K[5]$
- (2) for  $i = 0$  to 27:
  - $T[0] \leftarrow (T[0] \boxplus (\delta[i \bmod 6] \lll i)) \lll 1$
  - $T[1] \leftarrow (T[1] \boxplus (\delta[i \bmod 6] \lll (i+1))) \lll 3$
  - $T[2] \leftarrow (T[2] \boxplus (\delta[i \bmod 6] \lll (i+2))) \lll 6$
  - $T[3] \leftarrow (T[3] \boxplus (\delta[i \bmod 6] \lll (i+3))) \lll 11$
  - $T[4] \leftarrow (T[4] \boxplus (\delta[i \bmod 6] \lll (i+4))) \lll 13$
  - $T[5] \leftarrow (T[5] \boxplus (\delta[i \bmod 6] \lll (i+5))) \lll 17$
- $K_i \leftarrow T[0]||T[1]||T[2]||T[3]||T[4]||T[5]$

The key schedule procedure for LEA-192 is illustrated in Figure 14.

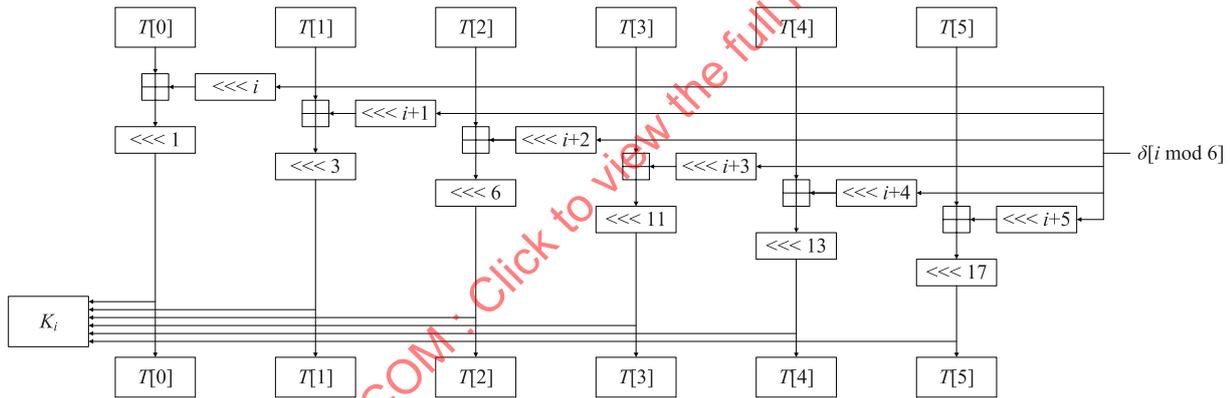


Figure 14 — The key schedule procedure for LEA-192

#### 6.3.5.4 Key schedule for LEA-256

Let  $K = K[0]||K[1]||K[2]||K[3]||K[4]||K[5]||K[6]||K[7]$  be a 256-bit key, where  $K[i] \in \{0,1\}^{32}$  ( $0 \leq i < 8$ ). The key schedule for LEA-256 takes  $K$  and the eight 32-bit constant values  $\delta[i]$  ( $0 \leq i < 8$ ) described in 6.3.5.5 as inputs and outputs thirty-two 192-bit round keys  $K_i$  ( $0 \leq i < 32$ ).

The key schedule operation for LEA-256 is as follows:

- (1)  $T[0]||T[1]||T[2]||T[3]||T[4]||T[5]||T[6]||T[7] \leftarrow K[0]||K[1]||K[2]||K[3]||K[4]||K[5]||K[6]||K[7]$
- (2) for  $i = 0$  to 31:
  - $T[6i \bmod 8] \leftarrow (T[6i \bmod 8] \boxplus (\delta[i \bmod 8] \lll i)) \lll 1$
  - $T[6i+1 \bmod 8] \leftarrow (T[6i+1 \bmod 8] \boxplus (\delta[i \bmod 8] \lll (i+1))) \lll 3$

$$T[6i+2 \bmod 8] \leftarrow (T[6i+2 \bmod 8] \boxplus (\delta[i \bmod 8] \lll (i+2))) \lll 6$$

$$T[6i+3 \bmod 8] \leftarrow (T[6i+3 \bmod 8] \boxplus (\delta[i \bmod 8] \lll (i+3))) \lll 11$$

$$T[6i+4 \bmod 8] \leftarrow (T[6i+4 \bmod 8] \boxplus (\delta[i \bmod 8] \lll (i+4))) \lll 13$$

$$T[6i+5 \bmod 8] \leftarrow (T[6i+5 \bmod 8] \boxplus (\delta[i \bmod 8] \lll (i+5))) \lll 17$$

$$K_i \leftarrow T[6i \bmod 8] \parallel T[6i+1 \bmod 8] \parallel T[6i+2 \bmod 8] \parallel T[6i+3 \bmod 8] \parallel T[6i+4 \bmod 8] \parallel T[6i+5 \bmod 8]$$

The key schedule procedure for LEA-256 is illustrated in Figure 15.

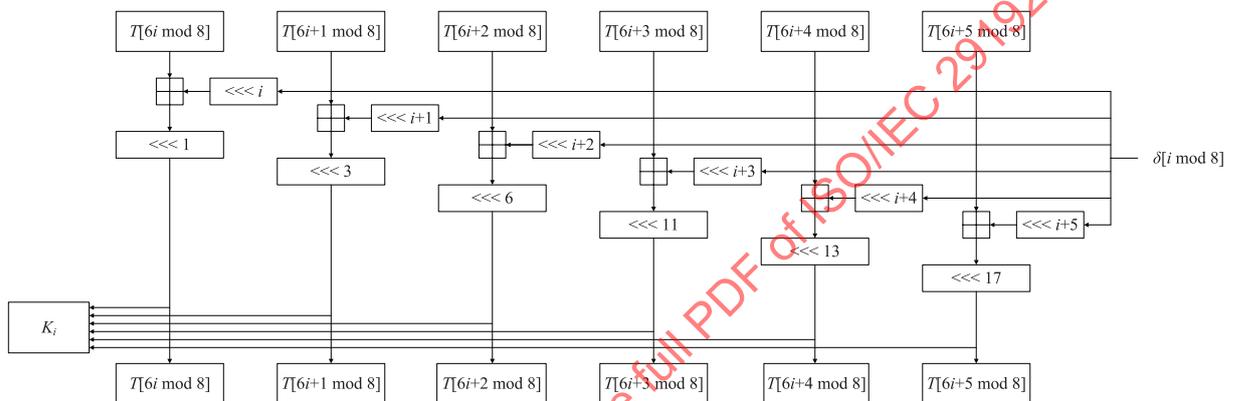


Figure 15 — The key schedule procedure for LEA-256

### 6.3.5.5 Constant values

The eight 32-bit constant values  $\delta[i]$  ( $0 \leq i < 8$ ) are used in the key schedule algorithm. They are the first 256 bits of the fractional part of  $\sqrt{766965}$ , where 76, 69, and 65 are ASCII codes of 'L', 'E', and 'A', respectively. They are given in Table 18.

Table 18 — Constant values used in the key schedule

| $i$ | $\delta[i]$ | $i$ | $\delta[i]$ |
|-----|-------------|-----|-------------|
| 0   | 0xc3efe9db  | 4   | 0x715ea49e  |
| 1   | 0x44626b02  | 5   | 0xc785da0a  |
| 2   | 0x79e27c8a  | 6   | 0xe04ef22a  |
| 3   | 0x78df30ec  | 7   | 0xe5c40957  |

## Annex A (normative)

### Object identifiers

This annex lists the object identifiers assigned to algorithms specified in this document.

```

--
-- ISO/IEC 29192-2 ASN.1 Module
--
LightweightCryptography-2 {
iso(1) standard(0) lightweight-cryptography(29192) part2(2)
asn1-module(0) algorithm-object-identifiers(0)}
DEFINITIONS EXPLICIT TAGS ::= BEGIN
-- EXPORTS All; --
-- IMPORTS None; --
OID ::= OBJECT IDENTIFIER -- Alias
-- Synonyms --
is29192-2 OID ::= {iso(1) standard(0) lightweight-cryptography(29192)
part2(2)}
id-lbc64 OID ::= {is29192-2 cipher-64-bit(1)}
id-lbc128 OID ::= {is29192-2 cipher-128-bit(2)}
-- Assignments --
id-bc64-present OID ::= {id-lbc64 present(1)}
id-bc128-clefiia OID ::= {id-lbc128 clefiia(1)}
id-bc128-lea OID ::= {id-lbc128 lea(2)}
LightweightCryptographyIdentifier ::= SEQUENCE {
algorithm ALGORITHM.&id({BlockAlgorithms}),
parameters ALGORITHM.&Type({BlockAlgorithms}{@algorithm}) OPTIONAL
}
BlockAlgorithms ALGORITHM ::= {
{ OID id-bc64-present PARMS KeyLengthID },
{ OID id-bc128-clefiia PARMS KeyLengthID },
{ OID id-bc128-lea PARMS KeyLengthID },
... -- Expect additional algorithms --
}
KeyLength ::= INTEGER
KeyLengthID ::= CHOICE {
int KeyLength,
oid OID
}
-- Cryptographic algorithm identification --
ALGORITHM ::= CLASS {
&id OBJECT IDENTIFIER UNIQUE,
&Type OPTIONAL
}
WITH SYNTAX {OID &id [PARMS &Type] }
END -- LightweightCryptography-2 --

```

## Annex B (informative)

### Numerical examples

This annex provides numerical examples for PRESENT, CLEFIA, and LEA for each key length in hexadecimal notation.

#### B.1 PRESENT numerical examples

##### B.1.1 PRESENT-80

| Round | Round Key Value  | After addRoundKey | After sLayer     | After pLayer     |
|-------|------------------|-------------------|------------------|------------------|
|       | Plaintext        | 0123456789abcdef  |                  |                  |
|       | Key              | 0123456789abcdef  |                  | 0123             |
|       | Ciphertext       | f8dd50531d973bde  |                  |                  |
| 1     | 0123456789abcdef | 0000000000000000  | cccccccccccccccc | ffffffff00000000 |
| 2     | 1024602468acf135 | efdb9fdb68acf135  | 1278e278a3f425b0 | 19a22a346eeaa266 |
| 3     | 8f37a2048c048d14 | 96958830e2ee2f72  | ea033bc161162d6  | e302a14bee4d0eb2 |
| 4     | e3c4d1e6f4409181 | 00c670ad1a0d9f33  | cc4adcf75fc7e2bb | de6bef8135f0bd3  |
| 5     | 62345c789a3cde8a | bc5fb3808963d559  | 84028b3c3eab700e | 8d71414916f90698 |
| 6     | 92460c468b8f1345 | 1f374d0f9d7615dd  | 52bd97c2e7da5077 | 3ab096eb65d3bc6b |
| 7     | f37a3248c188d172 | c9caa4a3a45b6d19  | 4e4ff9fbf908a75e | 5fd9fa875b8d1fc6 |
| 8     | 0c4d1e6f46491832 | 5394e4e81dc407f4  | 0be919135749cd29 | 741d20ec61425fd5 |
| 9     | 0345c189a3cde8cd | 7758e165c28fb718  | dd0315a046328d53 | c20cc4c61271dc27 |
| 10    | f460c068b831347d | 366c04aeaa40e85a  | baa4c9f1ff9c130f | eef11ad1e2c587ed |
| 11    | f7a33e8c180d1703 | 1952245dfac890ee  | 5e0669072f43ec11 | 444cd96c59d88553 |
| 12    | a4d1fef467d18304 | e09d27983e090657  | 1ce76de3b1ceca0d | 66bd7e393b9495c1 |
| 13    | 345c149a3fde8cfc | 52e16aa3044a193d  | 0615affbc99f5eb7 | 0ff6569d4f17377b |
| 14    | 360c068b829347fa | 39fa5016cd847086  | be2f0c5a4739dc3a | d51d56ccf163927a |
| 15    | fa33e6c180d17055 | 2f2eb00d71b2e22f  | 62618cc7d5861662 | 0ea0a7d6e11711c8 |
| 16    | fd1fff467cd8301d | f3bf58909dcf21d5  | 2b8203ece7426570 | 638003eed6da4446 |
| 17    | 85c15fa31fe8cf93 | e6415c4d29328bd5  | 1a9504976eb63870 | 626415d241fab32a |
| 18    | a0c070b82bf47ff5 | c2a4656a6a0eccdf  | 46f9a0afafc14472 | 3be0e16e6bc33152 |
| 19    | 833e54180e170577 | b8deb57665d43425  | 837180daa079b960 | 8b9c222261aa723c |
| 20    | 21ffd067ca8301cb | aa63f245ab2973f7  | ffab2690f86edb2d | f2ddc4b9fcb6d28d |
| 21    | ac15c43ffa0cf95a | 5ec8008606ba2bd7  | 0143cc3aca8f687d | 0df52c9b135a5213 |
| 22    | 9c073582b887ff4b | 91f21919abddad58  | e5265e5ef877f703 | 85c8dfbcb5bd4abd |
| 23    | a3e57380e6b0571b | 262dac3c530d1da6  | 6a67f4b40bc757fa | 4a63bd3efa571a5e |
| 24    | dffd347cae701cdd | 959e894254270683  | e0e13e96096dca3b | a65da538ad271a53 |
| 25    | 815c7bffa68f95c2 | 2701dec70ba88f91  | 6dc5714dc8f332e5 | 61e2fba3883e5d39 |
| 26    | 9073702b8f7ff4dd | f1918b880741a9e4  | 25e53833cd95fe19 | 24ed70dcab0c5b7b |
| 27    | fe57120e6e0571e2 | daba62d2c5092a99  | 7f8fa67640ce6fee | 7837d7bdfd1fd204 |
| 28    | 0fd37fcae241cdcd | 77e4a8753d5e1fc9  | dd19f3d0b701524e | da81ca4b0cc5fed8 |
| 29    | f5c781fa6ff95c46 | 2f464bb1633ca29e  | 629a9885abb4f6e1 | 3eea811ed0ee2969 |
| 30    | 47373eb8f03f4df1 | 79ddbfa620d16498  | de7782fa6c75a9e3 | cb4ef2f277abb235 |
| 31    | b57108e6e7d71e08 | 7e3ffa14907cac3d  | d1b22f59ecd4f4b7 | a5ea86fd3c8be72b |
| 32    | 5d37d6ae211cdcf5 | f8dd50531d973bde  |                  |                  |

**B.1.2 PRESENT-128**

| <b>Plaintext</b>  | <b>0123456789abcdef</b> |                   |                         |                  |
|-------------------|-------------------------|-------------------|-------------------------|------------------|
| <b>Key</b>        | <b>0011223344556677</b> |                   | <b>8899aabbccddeeff</b> |                  |
| <b>Ciphertext</b> | <b>88728500054418de</b> |                   |                         |                  |
| Round             | Round Key Value         | After addRoundKey | After sLayer            | After pLayer     |
| 1                 | 0011223344556677        | 01326754cdfcab98  | c5b6ad094721f8e3        | ad0ed4ca386b6559 |
| 2                 | 25133557799bbddf        | 881de19d41f0d886  | 335715e7952c733a        | 02913758d32ffdc  |
| 3                 | 29004488cd115599        | 2b9173d01e3ea857  | 68e5db7c51b1f30d        | 6d29bb89a62c1efd |
| 4                 | 63944cd55de66ef7        | 0ebdf75cfbca700a  | c1872d04284fdccf        | a45f953f18915419 |
| 5                 | 29a4011223344557        | 8dfb942d3ba5114e  | 3728e967b8f05591        | 1ce24b2ceba0c5af |
| 6                 | 178e5133557799ba        | 0b6c1a1fbed75c15  | c8a45f52817d0450        | e4909e362520e72  |
| 7                 | 0ca69004488cd114        | e8360e326dacdf66  | 13bac1b6a7f472aa        | 3aa3097873efe668 |
| 8                 | e35e3944cd55de67        | d9fd303cbeba380f  | 7e27bcb4818fb3c2        | 4ebad512fa1d9a5c |
| 9                 | 19329a4011223346        | 57884f52eb3fa91a  | 0d33920618b2fe5f        | 486d410f353d78ab |
| 10                | 488d78e51335577b        | 00e039ea26082fd0  | cc1cbelf6ac3627c        | dd61d5ab0dde2b12 |
| 11                | d364ca69004488cf        | 0e051fc20d9aa3dd  | c1c05246c7effb77        | a0bcabfb057f485f |
| 12                | 252235e3944cd55f        | 859e9e1891339d00  | 30e1e153e5bbe7cc        | 28bb2acfa9bc9774 |
| 13                | 1d4d9329a4011220        | 35f6b9e60dbd8554  | b02a8e1ac7873009        | 9da104d0b5588259 |
| 14                | c99488d78e513356        | 54358c073b09b10f  | 09b034cdb8ce85c2        | 63fa073628916984 |
| 15                | 4975364ca690044b        | 2a8f317a8e016dcf  | 6f32b5df31c5a742        | 4b28c736f98d6fd4 |
| 16                | ab2652235e3944ce        | e00e9515a7b42b1a  | 1cc1e050fd89685f        | 68f56acb088992d3 |
| 17                | 7525d4d9329a4015        | 1dd0be123a13d2c6  | 577c8156bf5b764a        | 18d1f36e61dde6f8 |
| 18                | faac99488d78e517        | e27d6a26eca503ef  | 16d7af6a14f0cb12        | 2d2c76685f25b4a6 |
| 19                | 17d4975364ca6904        | 3af8e13b3befdda2  | bf2315b8b81277f6        | c3c2440ff29fdeae |
| 20                | e8eab2652235e390        | 2b28f66ad0aa3d3e  | 68632aaf7cfff7b1        | 477aa1f4bfbellbf |
| 21                | 5c5f525d4d9329a1        | 1b25f3a9f22d381e  | 58602bfe2667b351        | 4708a3722ffc861f |
| 22                | 6ba3aac99488d78b        | 2cab09bbb745194   | 64f8ce8888d905e9        | 3ff3ec26a4022035 |
| 23                | a5717d4975364ca3        | 9a82916fd1346c96  | ef36e5a275b9a4ea        | ca3bdcc6fbab64f0 |
| 24                | a5ae8eab2652235b        | 6f95526dddf947ab  | a2e006a7772e9df8        | a21f25d6e7f201ce |
| 25                | d195c5f525d4d934        | 738ae023c226d8fa  | db3f1c6b466a732f        | d51196e9737ff90d |
| 26                | e696ba3aac99488b        | 33872cd3dfe6b186  | bb3d647b721a853a        | d1191e84ebd3f3a6 |
| 27                | ad465717d4975362        | 7c5f49933f44a0c4  | d4029eebb299fc49        | 8fbdc60e17c889b9 |
| 28                | 989a5ae8eab26524        | 17279ce6fd7aec9d  | 5d6de41a27df14e7        | 5932fc7729d3d279 |
| 29                | e1b5195c5f525d4a        | b887e52b76818f33  | 833d1068da3532bb        | 91c31290626f78bb |
| 30                | 0662696ba3aac993        | 97a17bfbcb1c5b128 | edf5d82845408563        | ed08f8e6a2037845 |
| 31                | d886d465717d4972        | 358e2c83d37e3137  | b031643b7bd1b5bd        | 816b0ca5abcab3ff |
| 32                | 091989a5ae8eab21        | 88728500054418de  |                         |                  |

**B.2 CLEFIA numerical examples**

**B.2.1 CLEFIA with a 128-bit key**

key                ffeeddcc bbaa9988 77665544 33221100

plaintext        00010203 04050607 08090a0b 0c0d0e0f

ciphertext       de2bf2fd 9b74aacd f1298555 459494fd

L                 8f89a61b 9db9d0f3 93e65627 da0d027e

*WK*<sub>0,1,2,3</sub> ffeeddcc bbaa9988 77665544 33221100  
*RK*<sub>0,1,2,3</sub> f3e6cef9 8df75e38 41c06256 640ac51b  
*RK*<sub>4,5,6,7</sub> 6a27e20a 5a791b90 e8c528dc 00336ea3  
*RK*<sub>8,9,10,11</sub> 59cd17c4 28565583 312a37cc c08abd77  
*RK*<sub>12,13,14,15</sub> 7e8e7eec 8be7e949 d3f463d6 a0aad6aa  
*RK*<sub>16,17,18,19</sub> e75eb039 0d657eb9 018002e2 9117d009  
*RK*<sub>20,21,22,23</sub> 9f98d11e babee8cf b0369efa d3aaef0d  
*RK*<sub>24,25,26,27</sub> 3438f93b f9cea4a0 68df9029 b869b4a7  
*RK*<sub>28,29,30,31</sub> 24d6406d e74bc550 41c28193 16de4795  
*RK*<sub>32,33,34,35</sub> a34a20f5 33265d14 b19d0554 5142f434

|                       |               |          |           |          |          |
|-----------------------|---------------|----------|-----------|----------|----------|
| plaintext             |               | 00010203 | 04050607  | 08090a0b | 0c0d0e0f |
| initial whitening key |               | ffeeddcc |           |          | bbaa9988 |
| after whitening       |               | 00010203 | fbebdbc b | 08090a0b | b7a79787 |
| Round 1               | input         | 00010203 | fbebdbc b | 08090a0b | b7a79787 |
|                       | F-function    | $F_0$    |           | $F_1$    |          |
|                       | input         | 00010203 |           | 08090a0b |          |
|                       | round key     | f3e6cef9 |           | 8df75e38 |          |
|                       | after key add | f3e7ccfa |           | 85fe5433 |          |
|                       | after S       | 290246e1 |           | 777de8e8 |          |
|                       | after M       | 547a3193 |           | abf12070 |          |
| Round 2               | input         | af91ea58 | 08090a0b  | 1c56b7f7 | 00010203 |
|                       | F-function    | $F_0$    |           | $F_1$    |          |
|                       | input         | af91ea58 |           | 1c56b7f7 |          |
|                       | round key     | 41c06256 |           | 640ac51b |          |
|                       | after key add | ee51880e |           | 785c72ec |          |
|                       | after S       | cb5d2b0c |           | 63a5edd2 |          |
|                       | after M       | f51cebb3 |           | 82dfe347 |          |
| Round 3               | input         | fd15e1b8 | 1c56b7f7  | 82dee144 | af91ea58 |
|                       | F-function    | $F_0$    |           | $F_1$    |          |
|                       | input         | fd15e1b8 |           | 82dee144 |          |
|                       | round key     | 6a27e20a |           | 5a791b90 |          |
|                       | after key add | 973203b2 |           | d8a7fad4 |          |
|                       | after S       | c2c7c6c2 |           | be59e10d |          |
|                       | after M       | d8dfd8de |           | e15ea81c |          |

|         |            |          |          |          |          |
|---------|------------|----------|----------|----------|----------|
| Round 4 | input      | c4896f29 | 82dee144 | 4ecf4244 | fd15e1b8 |
|         | F-function | $F_0$    |          | $F_1$    |          |
|         | input      | c4896f29 |          | 4ecf4244 |          |
|         | round key  | e8c528dc |          | 00336ea3 |          |
|         | after key  | 2c4c47f5 |          | 4efc2ce7 |          |
|         | add        | 9da4dafc |          | 43bce638 |          |
|         | after S    | b5b28e96 |          | b65c519a |          |
|         | after M    |          |          |          |          |
| Round 5 | input      | 376c6fd2 | 4ecf4244 | 4b49b022 | c4896f29 |
|         | F-function | $F_0$    |          | $F_1$    |          |
|         | input      | 376c6fd2 |          | 4b49b022 |          |
|         | round key  | 59cd17c4 |          | 28565583 |          |
|         | after key  | 6ea17816 |          | 631fe5a1 |          |
|         | add        | f26ad3e5 |          | 62af9f1b |          |
|         | after S    | 29f08afd |          | be01d127 |          |
|         | after M    |          |          |          |          |
| Round 6 | input      | 673fc8b9 | 4b49b022 | 7a88be0e | 376c6fd2 |
|         | F-function | $F_0$    |          | $F_1$    |          |
|         | input      | 673fc8b9 |          | 7a88be0e |          |
|         | round key  | 312a37cc |          | c08abd77 |          |
|         | after key  | 5615ff75 |          | ba020379 |          |
|         | add        | b39c8e58 |          | 2dd1e9a2 |          |
|         | after S    | 5999a79e |          | 0429b329 |          |
|         | after M    |          |          |          |          |
| Round 7 | input      | 12d017bc | 7a88be0e | 3345dcfb | 673fc8b9 |
|         | F-function | $F_0$    |          | $F_1$    |          |
|         | input      | 12d017bc |          | 3345dcfb |          |
|         | round key  | 7e8e7eec |          | 8be7e949 |          |
|         | after key  | 6c5e6950 |          | b8a235b2 |          |
|         | add        | 8b737025 |          | 67a08eba |          |
|         | after S    | 6ed11b09 |          | dfd3cd32 |          |
|         | after M    |          |          |          |          |
| Round 8 | input      | 1459a507 | 3345dcfb | b8ec058b | 12d017bc |
|         | F-function | $F_0$    |          | $F_1$    |          |
|         | input      | 1459a507 |          | b8ec058b |          |
|         | round key  | d3f463d6 |          | a0aad6aa |          |
|         | after key  | c7adc6d1 |          | 1846d321 |          |
|         | add        | e7ee5a5f |          | 9e97f1a1 |          |
|         | after S    | 8c9d011c |          | 93684eec |          |
|         | after M    |          |          |          |          |

|          |            |                   |                   |
|----------|------------|-------------------|-------------------|
| Round 9  | input      | bfd8dde7 b8ec058b | 81b85950 1459a507 |
|          | F-function | $F_0$             | $F_1$             |
|          | input      | bfd8dde7          | 81b85950          |
|          | round key  | e75eb039          | 0d657eb9          |
|          | after key  | 58866dde          | 8cdd27e9          |
|          | add        |                   |                   |
|          | after S    | 4e821daf          | 59c56044          |
|          | after M    | e6d6501e          | 6d5839b4          |
| Round 10 | input      | 5e3a5595 81b85950 | 79019cb3 bfd8dde7 |
|          | F-function | $F_0$             | $F_1$             |
|          | input      | 5e3a5595          | 79019cb3          |
|          | round key  | 018002e2          | 9117d009          |
|          | after key  | 5fba5777          | e8164cba          |
|          | add        |                   |                   |
|          | after S    | 612d8f7b          | 0185a49c          |
|          | after M    | 3a1b0e97          | b9b479c8          |
| Round 11 | input      | bba357c7 79019cb3 | 066ca42f 5e3a5595 |
|          | F-function | $F_0$             | $F_1$             |
|          | input      | bba357c7          | 066ca42f          |
|          | round key  | 9f98d11e          | babee8cf          |
|          | after key  | 243b86d9          | bcd24ce0          |
|          | add        |                   |                   |
|          | after S    | f70f1144          | cb72a481          |
|          | after M    | 28974052          | 4a6700b1          |
| Round 12 | input      | 5196dce1 066ca42f | 145d5524 bba357c7 |
|          | F-function | $F_0$             | $F_1$             |
|          | input      | 5196dce1          | 145d5524          |
|          | round key  | b0369efa          | d3aaef0d          |
|          | after key  | e1a0421b          | c7f7ba29          |
|          | add        |                   |                   |
|          | after S    | 6f7efd4f          | 72642dce          |
|          | after M    | ffb5db32          | 907d3820          |
| Round 13 | input      | f9d97f1d 145d5524 | 2bde6fe7 5196dce1 |
|          | F-function | $F_0$             | $F_1$             |
|          | input      | f9d97f1d          | 2bde6fe7          |
|          | round key  | 3438f93b          | f9cea4a0          |
|          | after key  | cde18626          | d210cb47          |
|          | add        |                   |                   |
|          | after S    | 3f751141          | ab28e0da          |
|          | after M    | 0a744c28          | 1c3e38a3          |

|          |                     |          |          |          |          |
|----------|---------------------|----------|----------|----------|----------|
| Round 14 | input               | 1e29190c | 2bde6fe7 | 4da8e442 | f9d97f1d |
|          | F-function          | $F_0$    |          | $F_1$    |          |
|          | input               | 1e29190c |          | 4da8e442 |          |
|          | round key           | 68df9029 |          | b869b4a7 |          |
|          | after key add       | 76f68925 |          | f5c150e5 |          |
|          | after S             | fe6db7e7 |          | fc0c25f6 |          |
|          | after M             | aaa2c803 |          | c4315b8d |          |
| Round 15 | input               | 817ca7e4 | 4da8e442 | 3de82490 | 1e29190c |
|          | F-function          | $F_0$    |          | $F_1$    |          |
|          | input               | 817ca7e4 |          | 3de82490 |          |
|          | round key           | 24d6406d |          | e74bc550 |          |
|          | after key add       | a5aae789 |          | daa3e1c0 |          |
|          | after S             | 8d233818 |          | 2904757b |          |
|          | after M             | 7bd4cced |          | eac2f0fb |          |
| Round 16 | input               | 367c28af | 3de82490 | f4ebe9f7 | 817ca7e4 |
|          | F-function          | $F_0$    |          | $F_1$    |          |
|          | input               | 367c28af |          | f4ebe9f7 |          |
|          | round key           | 41c28193 |          | 16de4795 |          |
|          | after key add       | 77bea93c |          | e235ae62 |          |
|          | after S             | 7c4a935b |          | 669b8953 |          |
|          | after M             | 598e6940 |          | c119609f |          |
| Round 17 | input               | 64664dd0 | f4ebe9f7 | 4065c77b | 367c28af |
|          | F-function          | $F_0$    |          | $F_1$    |          |
|          | input               | 64664dd0 |          | 4065c77b |          |
|          | round key           | a34a20f5 |          | 33265d14 |          |
|          | after key add       | c72c6d25 |          | 73439a6f |          |
|          | after S             | e7e61de7 |          | 788c85b4 |          |
|          | after M             | 2ac01b0a |          | c755adfa |          |
| Round 18 | input               | de2bf2fd | 4065c77b | f1298555 | 64664dd0 |
|          | F-function          | $F_0$    |          | $F_1$    |          |
|          | input               | de2bf2fd |          | f1298555 |          |
|          | round key           | b19d0554 |          | 5142f434 |          |
|          | after key add       | 6fb6f7a9 |          | a06b7161 |          |
|          | after S             | b44d648c |          | 7e99ea2a |          |
|          | after M             | ac7738f2 |          | 12d0c82d |          |
|          | output              | de2bf2fd | ec12ff89 | f1298555 | 76b685fd |
|          | final whitening key | 77665544 |          | 33221100 |          |
|          | after whitening     | de2bf2fd | 9b74aacd | f1298555 | 459494fd |
|          | ciphertext          | de2bf2fd | 9b74aacd | f1298555 | 459494fd |

STANDARDSISO.COM: Click to view the full PDF of ISO/IEC 29192-2:2019

**B.2.2 CLEFIA with a 192-bit key**

```

key          ffeeddcc bbaa9988 77665544 33221100
            f0e0d0c0 b0a09080

plaintext    00010203 04050607 08090a0b 0c0d0e0f

ciphertext   e2482f64 9f028dc4 80dda184 fde181ad

LL         db05415a 800082db 7cb8186c d788c5f3
LR         1ca9b2e1 b4606829 c92dd35e 2258a432

WK0,1,2,3    0f0e0d0c 0b0a0908 77777777 77777777
RK0,1,2,3    4d3bfd1b 7a1f5dfa 0fae6e7c c8bf3237
RK4,5,6,7    73c2eeb8 dd429ec5 e220b3af c9135e73
RK8,9,10,11  38c46a07 fc2ce4ba 370abf2d b05e627b
RK12,13,14,15 38351b2f 74bd6e1e 1b7c7dce 92cfc98e
RK16,17,18,19 509b31a6 4c5ad53c 6fc2ba33 e1e5c878
RK20,21,22,23 419a74b9 1dd79e0e 240a33d2 9dabfd09
RK24,25,26,27 6e3ff82a 74ac3ffd b9696e2e cc0b3a38
RK28,29,30,31 ed785cbd 9c077c13 04978d83 2ec058ba
RK32,33,34,35 4bbd5f6a 31fe8de8 b76da574 3a6fa8e7
RK36,37,38,39 521213ce 4f1f59d8 c13624f6 ee91f6a4
RK40,41,42,43 17f68fde f6c360a9 6288bc72 c0ad856b
    
```

|                       |               |                       |          |                       |          |
|-----------------------|---------------|-----------------------|----------|-----------------------|----------|
| plaintext             |               | 00010203              | 04050607 | 08090a0b              | 0c0d0e0f |
| initial whitening key |               | 0f0e0d0c              |          |                       | 0b0a0908 |
| after whitening       |               | 00010203              | 0b0b0b0b | 08090a0b              | 07070707 |
| Round 1               | input         | 00010203              | 0b0b0b0b | 08090a0b              | 07070707 |
|                       | F-function    | <i>F</i> <sub>0</sub> |          | <i>F</i> <sub>1</sub> |          |
|                       | input         | 00010203              |          | 08090a0b              |          |
|                       | round key     | 4d3bfd1b              |          | 7a1f5dfa              |          |
|                       | after key add | 4d3aff18              |          | 721657f1              |          |
|                       | after S       | 43c58e9e              |          | ed85d736              |          |
|                       | after M       | b5021a3b              |          | c397f62b              |          |

|         |            |          |          |          |          |
|---------|------------|----------|----------|----------|----------|
| Round 2 | input      | be091130 | 08090a0b | c490f12c | 00010203 |
|         | F-function | $F_0$    |          | $F_1$    |          |
|         | input      | be091130 |          | c490f12c |          |
|         | round key  | 0fae6e7c |          | c8bf3237 |          |
|         | after key  | b1a77f4c |          | 0c2fc31b |          |
|         | add        | f3d10ba4 |          | 13d83a3d |          |
|         | after S    | 9fba69c1 |          | 6683cae3 |          |
|         | after M    |          |          |          |          |
| Round 3 | input      | 97b363ca | c490f12c | 6682c8e0 | be091130 |
|         | F-function | $F_0$    |          | $F_1$    |          |
|         | input      | 97b363ca |          | 6682c8e0 |          |
|         | round key  | 73c2eeb8 |          | dd429ec5 |          |
|         | after key  | e4718d72 |          | bbc05625 |          |
|         | add        | 79ea66ed |          | f47b0d7a |          |
|         | after S    | 61c21ea5 |          | 120e06e2 |          |
|         | after M    |          |          |          |          |
| Round 4 | input      | a552ef89 | 6682c8e0 | ac0717d2 | 97b363ca |
|         | F-function | $F_0$    |          | $F_1$    |          |
|         | input      | a552ef89 |          | ac0717d2 |          |
|         | round key  | e220b3af |          | c9135e73 |          |
|         | after key  | 47725c26 |          | 651449a1 |          |
|         | add        | daeda541 |          | 355c651b |          |
|         | after S    | 28a43c63 |          | cb1ab573 |          |
|         | after M    |          |          |          |          |
| Round 5 | input      | 4e26f483 | ac0717d2 | 5ca9d6b9 | a552ef89 |
|         | F-function | $F_0$    |          | $F_1$    |          |
|         | input      | 4e26f483 |          | 5ca9d6b9 |          |
|         | round key  | 38c46a07 |          | fc2ce4ba |          |
|         | after key  | 76e29e84 |          | a0853203 |          |
|         | add        | fe663e39 |          | 7edcc7c6 |          |
|         | after S    | 5ce7dafe |          | ac7f4e3e |          |
|         | after M    |          |          |          |          |
| Round 6 | input      | f0e0cd2c | 5ca9d6b9 | 092da1b7 | 4e26f483 |
|         | F-function | $F_0$    |          | $F_1$    |          |
|         | input      | f0e0cd2c |          | 092da1b7 |          |
|         | round key  | 370abf2d |          | b05e627b |          |
|         | after key  | c7ea7201 |          | b973c3cc |          |
|         | add        | e77f9fda |          | 174a3a46 |          |
|         | after S    | b9869270 |          | 8fc7e089 |          |
|         | after M    |          |          |          |          |

|          |               |                   |                   |
|----------|---------------|-------------------|-------------------|
| Round 7  | input         | e52f44c9 092da1b7 | c1e1140a f0e0cd2c |
|          | F-function    | $F_0$             | $F_1$             |
|          | input         | e52f44c9          | c1e1140a          |
|          | round key     | 38351b2f          | 74bd6e1e          |
|          | after key add | dd1a5fe6          | b55c7a14          |
|          | after S       | c5496150          | 5aa5c15c          |
|          | after M       | 33d8590f          | e62eb913          |
| Round 8  | input         | 3af5f8b8 c1e1140a | 16ce743f e52f44c9 |
|          | F-function    | $F_0$             | $F_1$             |
|          | input         | 3af5f8b8          | 16ce743f          |
|          | round key     | 1b7c7dce          | 92cfc98e          |
|          | after key add | 21898576          | 8401bdb1          |
|          | after S       | a118dc09          | 3949b1f3          |
|          | after M       | f091202d          | 04f9e827          |
| Round 9  | input         | 31703427 16ce743f | e1d6acee 3af5f8b8 |
|          | F-function    | $F_0$             | $F_1$             |
|          | input         | 31703427          | e1d6acee          |
|          | round key     | 509b31a6          | 4c5ad53c          |
|          | after key add | 61eb0581          | ad8c79d2          |
|          | after S       | 2a8d3304          | eeffc072          |
|          | after M       | f9639a90          | 8bebfe3d          |
| Round 10 | input         | efadeeaf e1d6acee | b11e0685 31703427 |
|          | F-function    | $F_0$             | $F_1$             |
|          | input         | efadeeaf          | b11e0685          |
|          | round key     | 6fc2ba33          | e1e5c878          |
|          | after key add | 806f549c          | 50fbcefd          |
|          | after S       | cd5eeb61          | 25d7fe02          |
|          | after M       | a100e35b          | 26a4e16d          |
| Round 11 | input         | 40d64fb5 b11e0685 | 17d4d54a efadeeaf |
|          | F-function    | $F_0$             | $F_1$             |
|          | input         | 40d64fb5          | 17d4d54a          |
|          | round key     | 419a74b9          | 1dd79e0e          |
|          | after key add | 014c3b0c          | 0a034b44          |
|          | after S       | 49a4c013          | b4c6c912          |
|          | after M       | 51c0208f          | f1a2c339          |

|          |               |                   |                   |
|----------|---------------|-------------------|-------------------|
| Round 12 | input         | e0de260a 17d4d54a | 1e0f2d96 40d64fb5 |
|          | F-function    | $F_0$             | $F_1$             |
|          | input         | e0de260a          | 1e0f2d96          |
|          | round key     | 240a33d2          | 9dabfd09          |
|          | after key add | c4d415d8          | 83a4d09f          |
|          | after S       | 801beebe          | 86b8f8ed          |
|          | after M       | 8a9aef34          | 3e451646          |
| Round 13 | input         | 9d4e3a7e 1e0f2d96 | 7e9359f3 e0de260a |
|          | F-function    | $F_0$             | $F_1$             |
|          | input         | 9d4e3a7e          | 7e9359f3          |
|          | round key     | 6e3ff82a          | 74ac3ffd          |
|          | after key add | f371c254          | 0a3f660e          |
|          | after S       | 29ea68e8          | b4f530a8          |
|          | after M       | 17524741          | 4b8c607e          |
| Round 14 | input         | 095d6ad7 7e9359f3 | ab524674 9d4e3a7e |
|          | F-function    | $F_0$             | $F_1$             |
|          | input         | 095d6ad7          | ab524674          |
|          | round key     | b9696e2e          | cc0b3a38          |
|          | after key add | b03404f9          | 67597c4c          |
|          | after S       | 152a2f03          | 52161e39          |
|          | after M       | f7ee818b          | 7902f3eb          |
| Round 15 | input         | 897dd878 ab524674 | e44cc995 095d6ad7 |
|          | F-function    | $F_0$             | $F_1$             |
|          | input         | 897dd878          | e44cc995          |
|          | round key     | ed785cbd          | 9c077c13          |
|          | after key add | 640584c5          | 784bb586          |
|          | after S       | 459d9e10          | 636b5a11          |
|          | after M       | 4034defc          | 0228bdd4          |
| Round 16 | input         | eb669888 e44cc995 | 0b75d703 897dd878 |
|          | F-function    | $F_0$             | $F_1$             |
|          | input         | eb669888          | 0b75d703          |
|          | round key     | 04978d83          | 2ec058ba          |
|          | after key add | eff1150b          | 25b58fb9          |
|          | after S       | 90e4ee38          | e7691f3b          |
|          | after M       | 4a678609          | 05b2b4a9          |

|          |               |                   |                   |
|----------|---------------|-------------------|-------------------|
| Round 17 | input         | ae2b4f9c 0b75d703 | 8ccf6cd1 eb669888 |
|          | F-function    | $F_0$             | $F_1$             |
|          | input         | ae2b4f9c          | 8ccf6cd1          |
|          | round key     | 4bbd5f6a          | 31fe8de8          |
|          | after key add | e59610f6          | bd31e139          |
|          | after S       | f6a5286d          | b15d7589          |
|          | after M       | 720df49d          | bad65e22          |
| Round 18 | input         | 7978239e 8ccf6cd1 | 51b0c6aa ae2b4f9c |
|          | F-function    | $F_0$             | $F_1$             |
|          | input         | 7978239e          | 51b0c6aa          |
|          | round key     | b76da574          | 3a6fa8e7          |
|          | after key add | ce1586ea          | 6bdf6e4d          |
|          | after S       | 919c117f          | 283aaa43          |
|          | after M       | ef24fe56          | 08916103          |
| Round 19 | input         | 63eb9287 51b0c6aa | a6ba2e9f 7978239e |
|          | F-function    | $F_0$             | $F_1$             |
|          | input         | 63eb9287          | a6ba2e9f          |
|          | round key     | 521213ce          | 4f1f59d8          |
|          | after key add | 31f98149          | e9a57747          |
|          | after S       | 5d03e265          | 3c8d7bda          |
|          | after M       | b7464b63          | e1d086a7          |
| Round 20 | input         | e6f68dc9 a6ba2e9f | 98a8a539 63eb9287 |
|          | F-function    | $F_0$             | $F_1$             |
|          | input         | e6f68dc9          | 98a8a539          |
|          | round key     | c13624f6          | ee91f6a4          |
|          | after key add | 27c0a93f          | 7639539d          |
|          | after S       | 20b5938b          | 09893194          |
|          | after M       | 3cae819e          | b603c454          |
| Round 21 | input         | 9a14af01 98a8a539 | d5e856d3 e6f68dc9 |
|          | F-function    | $F_0$             | $F_1$             |
|          | input         | 9a14af01          | d5e856d3          |
|          | round key     | 17f68fde          | f6c360a9          |
|          | after key add | 8de220df          | 232b367a          |
|          | after S       | 6666bff2          | b383a1bd          |
|          | after M       | 7ae08a5d          | 662b2c4d          |

|          |                     |          |          |          |          |
|----------|---------------------|----------|----------|----------|----------|
| Round 22 | input               | e2482f64 | d5e856d3 | 80dda184 | 9a14af01 |
|          | F-function          | $F_0$    |          | $F_1$    |          |
|          | input               | e2482f64 |          | 80dda184 |          |
|          | round key           | 6288bc72 |          | c0ad856b |          |
|          | after key add       | 80c09316 |          | 407024ef |          |
|          | after S             | cdb5f1e5 |          | fbe99290 |          |
|          | after M             | 3d9dac60 |          | 108259db |          |
|          | output              | e2482f64 | e875fab3 | 80dda184 | 8a96f6da |
|          | final whitening key | 77777777 |          |          | 77777777 |
|          | after whitening     | e2482f64 | 9f028dc4 | 80dda184 | fde181ad |
|          | ciphertext          | e2482f64 | 9f028dc4 | 80dda184 | fde181ad |

**B.2.3 CLEFIA with a 256-bit key**

key            ffeeddcc bbba9988 77665544 33221100

                 f0e0d0c0 b0a09080 70605040 30201000

plaintext    00010203 04050607 08090a0b 0c0d0e0f

ciphertext   a1397814 289de80c 10da46d1 fa48b38a

$L_L$             477e8f09 66ee5378 2cc2be04 bf55e28f

$L_R$             d6c10b89 4eeab575 84bd5663 cc933940

$WK_{0,1,2,3}$     0f0e0d0c 0b0a0908 07060504 03020100

$RK_{0,1,2,3}$     58f02029 15413cd0 1b0c41a4 e4bacd0f

$RK_{4,5,6,7}$     6c498393 8846231b 1fc716fc 7c81a45b

$RK_{8,9,10,11}$   fa37c259 0e3da2ee aacf9abb 8ec0aad9

$RK_{12,13,14,15}$  b05bd737 8de1f2d0 8ffee0f6 b70b47ea

$RK_{16,17,18,19}$  581b3e34 03263f89 2f7100cd 05cee171

$RK_{20,21,22,23}$  b523d4e9 176d7c44 6d7ba5d7 f797b2f3

$RK_{24,25,26,27}$  25d80df2 a646bba2 6a3a95e1 3e3a47f0

$RK_{28,29,30,31}$  b304eb20 44f8824e c7557cbc 47401e21

$RK_{32,33,34,35}$  d71ff7e9 aca1fb0c 2deff35d 6ca3a830

$RK_{36,37,38,39}$  4dd7cfb7 ae71c9f6 4e911fef 90aa95de

$RK_{40,41,42,43}$  2c664a7a 8cb5cf6b 14c8de1e 43b9caef  
 $RK_{44,45,46,47}$  568c5a33 07ef7ddd 608dc860 ac9e50f8  
 $RK_{48,49,50,51}$  c0c18358 4f53c80e 33e01cb9 80251e1c

|                       |               |          |          |          |          |
|-----------------------|---------------|----------|----------|----------|----------|
| plaintext             |               | 00010203 | 04050607 | 08090a0b | 0c0d0e0f |
| initial whitening key |               | 0f0e0d0c |          |          | 0b0a0908 |
| after whitening       |               | 00010203 | 0b0b0b0b | 08090a0b | 07070707 |
| Round 1               | input         | 00010203 | 0b0b0b0b | 08090a0b | 07070707 |
|                       | F-function    | $F_0$    |          | $F_1$    |          |
|                       | input         | 00010203 |          | 08090a0b |          |
|                       | round key     | 58f02029 |          | 15413cd0 |          |
|                       | after key add | 58f1222a |          | 1d4836db |          |
|                       | after S       | 4ee41927 |          | 2c78a1ac |          |
|                       | after M       | 2db2101b |          | d87ee718 |          |
| Round 2               | input         | 26b91b10 | 08090a0b | df79e01f | 00010203 |
|                       | F-function    | $F_0$    |          | $F_1$    |          |
|                       | input         | 26b91b10 |          | df79e01f |          |
|                       | round key     | 1b0c41a4 |          | e4bacd0f |          |
|                       | after key add | 3db55ab4 |          | 3bc32d10 |          |
|                       | after S       | aa5afadb |          | 0f1e1928 |          |
|                       | after M       | 317e029c |          | c0cc96ba |          |
| Round 3               | input         | 39770897 | df79e01f | c0cd94b9 | 26b91b10 |
|                       | F-function    | $F_0$    |          | $F_1$    |          |
|                       | input         | 39770897 |          | c0cd94b9 |          |
|                       | round key     | 6c498393 |          | 8846231b |          |
|                       | after key add | 553e8b04 |          | 488bb7a2 |          |
|                       | after S       | 5487484e |          | d84876a0 |          |
|                       | after M       | c3a7ac1d |          | 7ae05884 |          |
| Round 4               | input         | 1cde4c02 | c0cd94b9 | 5c594394 | 39770897 |
|                       | F-function    | $F_0$    |          | $F_1$    |          |
|                       | input         | 1cde4c02 |          | 5c594394 |          |
|                       | round key     | 1fc716fc |          | 7c81a45b |          |
|                       | after key add | 03195afe |          | 20d8e7cf |          |
|                       | after S       | c607fa95 |          | 12f002c9 |          |
|                       | after M       | 5edee0ce |          | 4cfb0e90 |          |

|         |            |                   |                   |
|---------|------------|-------------------|-------------------|
| Round 5 | input      | 9e137477 5c594394 | 758c0607 1cde4c02 |
|         | F-function | $F_0$             | $F_1$             |
|         | input      | 9e137477          | 758c0607          |
|         | round key  | fa37c259          | 0e3da2ee          |
|         | after key  | 6424b62e          | 7bb1a4e9          |
|         | add        |                   |                   |
|         | after S    | 4592c8d2          | 46f3a044          |
|         | after M    | adfd33ae          | 42450650          |
| Round 6 | input      | f1a4703a 758c0607 | 5e9b4a52 9e137477 |
|         | F-function | $F_0$             | $F_1$             |
|         | input      | f1a4703a          | 5e9b4a52          |
|         | round key  | aacf9abb          | 8ec0aad9          |
|         | after key  | 5b6bea81          | d05be08b          |
|         | add        |                   |                   |
|         | after S    | 22285e04          | f822d448          |
|         | after M    | 0fa52ed4          | aa7a0a9c          |
| Round 7 | input      | 7a2928d3 5e9b4a52 | 34697eeb f1a4703a |
|         | F-function | $F_0$             | $F_1$             |
|         | input      | 7a2928d3          | 34697eeb          |
|         | round key  | b05bd737          | 8de1f2d0          |
|         | after key  | ca72ffe4          | b9888c3b          |
|         | add        |                   |                   |
|         | after S    | 23ed8e68          | 172b59c0          |
|         | after M    | 8b158630          | 334e2af2          |
| Round 8 | input      | d58ecc62 34697eeb | c2ea5ac8 7a2928d3 |
|         | F-function | $F_0$             | $F_1$             |
|         | input      | d58ecc62          | c2ea5ac8          |
|         | round key  | 8ffee0f6          | b70b47ea          |
|         | after key  | 5a702c94          | 75e11d22          |
|         | add        |                   |                   |
|         | after S    | facf9d64          | 586f2c19          |
|         | after M    | 72c2027e          | a582d5f0          |
| Round 9 | input      | 46ab7c95 c2ea5ac8 | dfabfd23 d58ecc62 |
|         | F-function | $F_0$             | $F_1$             |
|         | input      | 46ab7c95          | dfabfd23          |
|         | round key  | 581b3e34          | 03263f89          |
|         | after key  | 1eb042a1          | dc8dc2aa          |
|         | add        |                   |                   |
|         | after S    | 177afd6a          | 57664735          |
|         | after M    | 51d5740a          | 110287d7          |

|          |               |          |          |          |          |
|----------|---------------|----------|----------|----------|----------|
| Round 10 | input         | 933f2ec2 | dfabfd23 | c48c4bb5 | 46ab7c95 |
|          | F-function    | $F_0$    |          | $F_1$    |          |
|          | input         | 933f2ec2 |          | c48c4bb5 |          |
|          | round key     | 2f7100cd |          | 05cee171 |          |
|          | after key add | bc4e2e0f |          | c142aac4 |          |
|          | after S       | e0434cd9 |          | 22fd2380 |          |
|          | after M       | a768d32a |          | b6ae4f2b |          |
| Round 11 | input         | 78c32e09 | c48c4bb5 | f00533be | 933f2ec2 |
|          | F-function    | $F_0$    |          | $F_1$    |          |
|          | input         | 78c32e09 |          | f00533be |          |
|          | round key     | b523d4e9 |          | 176d7c44 |          |
|          | after key add | cde0fae0 |          | e7684ffa |          |
|          | after S       | 3fd410d4 |          | 02ef5310 |          |
|          | after M       | 08bd9b01 |          | 2fdb3f65 |          |
| Round 12 | input         | cc31d0b4 | f00533be | bce411a7 | 78c32e09 |
|          | F-function    | $F_0$    |          | $F_1$    |          |
|          | input         | cc31d0b4 |          | bce411a7 |          |
|          | round key     | 6d7ba5d7 |          | f797b2f3 |          |
|          | after key add | a14a7563 |          | 4b73a354 |          |
|          | after S       | 1b512562 |          | c94a71eb |          |
|          | after M       | 7c2a762b |          | 81ca0b59 |          |
| Round 13 | input         | 8c294595 | bce411a7 | f9092550 | cc31d0b4 |
|          | F-function    | $F_0$    |          | $F_1$    |          |
|          | input         | 8c294595 |          | f9092550 |          |
|          | round key     | 25d80df2 |          | a646bba2 |          |
|          | after key add | a9f14867 |          | 5f4f9ef2 |          |
|          | after S       | 93e47852 |          | 5c26cae5 |          |
|          | after M       | 4a87c858 |          | 54bc68d5 |          |
| Round 14 | input         | f663d9ff | f9092550 | 988db861 | 8c294595 |
|          | F-function    | $F_0$    |          | $F_1$    |          |
|          | input         | f663d9ff |          | 988db861 |          |
|          | round key     | 6a3a95e1 |          | 3e3a47f0 |          |
|          | after key add | 9c594c1e |          | a6b7ff91 |          |
|          | after S       | 58ff39b0 |          | 054d1d75 |          |
|          | after M       | d82301d4 |          | 085d5025 |          |