BS ISO/IEC 29192-2:2019

BSI Standards Publication

Information security — Lightweight cryptography

Part 2: Block ciphers

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 29192-2:2019

National foreword

This British Standard is the UK implementation of ISO/IEC 29192-2:2019. It supersedes BS ISO/IEC 29192-2:2012, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, Security, cybersecurity and privacy protection.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2019
Published by BSI Standards Limited 2019

ISBN 978 0 539 05015 8

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2019.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 29192-2:2019

INTERNATIONAL STANDARD

ISO/IEC 29192-2

Second edition
2019-11

Information security — Lightweight cryptography —

Part 2: Block ciphers

Sécurité de l'information — Cryptographie pour environnements contraints —

Partie 2: Chiffrements par blocs

Reference number
ISO/IEC 29192-2:2019(E)

Documents
Document Sharing Hub
© ISO/IEC 2019

Full document details: BS 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
Website: www.iso.org

Published in Switzerland

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 29192-2:2019

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Symbols ... **2**
5 Lightweight block cipher with a block size of 64 bits ... **2**
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
6 Lightweight block ciphers with a block size of 128 bits ... **7**
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
Annex A (normative) **Object identifiers** ... **30**
Annex B (informative) **Numerical examples** ... **31**
Annex C (informative) **Feature tables** ... **53**
Annex D (informative) **A limitation of a block cipher under a single key** ... **55**
Bibliography ... **56**

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29192-2:2019

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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www. iso. org/patents) or the IEC list of patent declarations received (see 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.

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.

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.

© ISO/IEC 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29192-2:2019

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.

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.

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29192-2:2019

Documents
Document Sharing Hub

Full document details: BS 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]

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29192-2:2019

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

`0x`	a prefix for a binary string in hexadecimal notation
$\|\|$	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[10] 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

$K_i = k^i_{63} \ldots k^i_0$	64-bit round key that is used in round i
k^i_b	bit b of round key K_i
$K = k_{79} \ldots k_0$	80-bit key register
k_b	bit b of key register K

© ISO/IEC 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29192-2:2019

STATE	64-bit internal state
b_i	bit i of the current *STATE*
w_i	4-bit word where $0 \le i \le 15$

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 ($1 \le i \le 31$), 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)
```

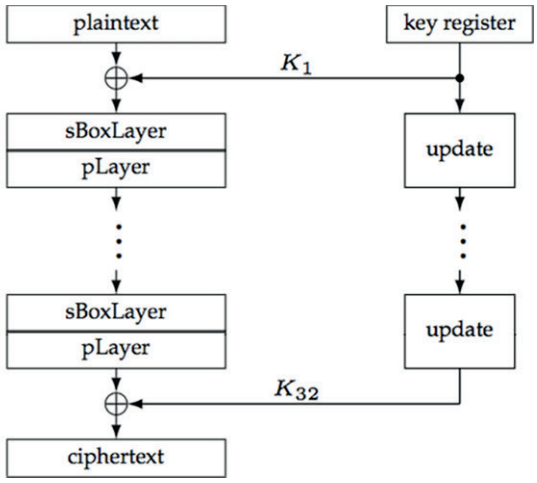

Figure 1 — The encryption procedure of PRESENT

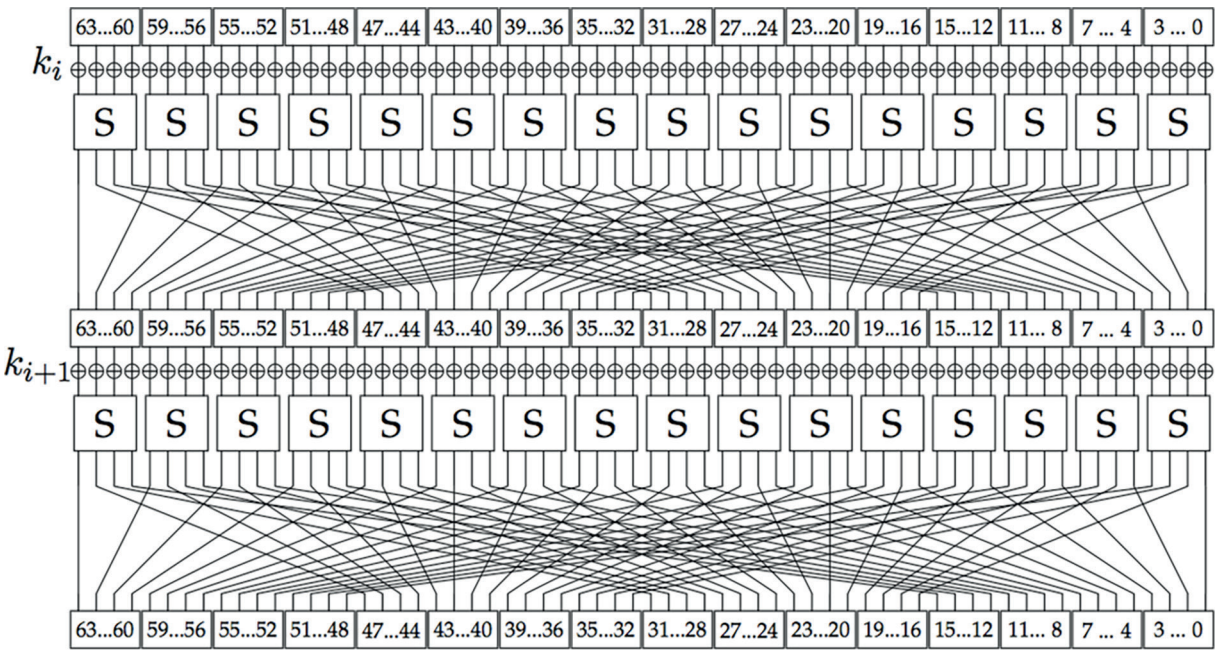

Figure 2 — Two rounds of PRESENT

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29192-2:2019

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 ($1 \le i \le 31$), 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
```

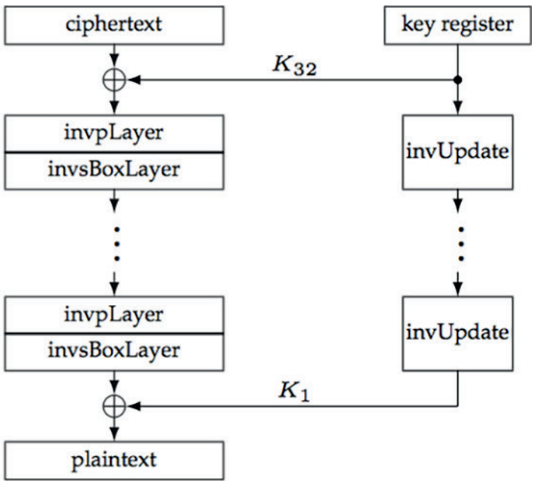

Figure 3 — The decryption procedure of PRESENT

5.2.5 PRESENT transformations

5.2.5.1 addRoundKey

Given round key $K_i = k^i_{63} \ldots k^i_0$ for $1 \le i \le 32$ and current *STATE* $b_{63} \ldots b_0$, **addRoundKey** consists of the operation for $0 \le j \le 63$, $b_j \leftarrow b_j \oplus k^i_j$.

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

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

© ISO/IEC 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29192-2:2019

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.

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29192-2:2019

5.2.6.2 80-bit key for PRESENT-80

The user-supplied key is stored in a key register K and represented as $k_{79}k_{78}...k_0$. At round i the 64-bit round key $K_i = k^i_{63}k^i_{62}\ldots k^i_0$ consists of the 64 leftmost bits of the current contents of register K. Thus at round i, K_i is as follows:

$$K_i = k^i_{63}k^i_{62}\ldots k^i_0 = k_{79}k_{78}\ldots k_{16}$$

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

1) $k_{79}k_{78}...k_1k_0 \leftarrow k_{18}k_{17}...k_{20}k_{19}$

2) $k_{79}k_{78}k_{77}k_{76} \leftarrow S[k_{79}k_{78}k_{77}k_{76}]$

3) $k_{19}k_{18}k_{17}k_{16}k_{15} \leftarrow k_{19}k_{18}k_{17}k_{16}k_{15} \oplus round_counter$

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 $1 \le i \le 31$ and *round_counter* = i. Figure 4 depicts the key schedule for PRESENT-80 graphically.

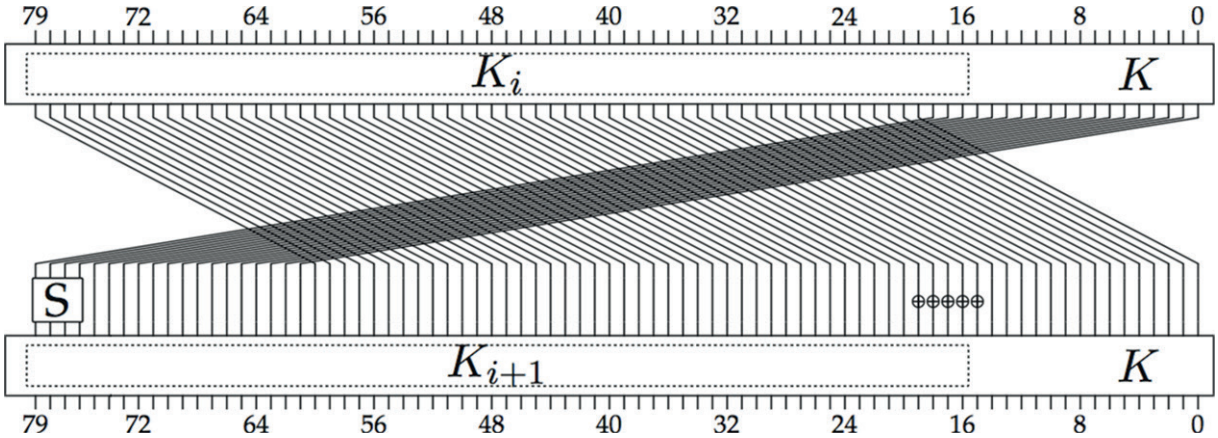

Figure 4 — PRESENT-80 key schedule

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 $k_{127}k_{126}...k_0$. At round i the 64-bit round key $K_i = k^i_{63}k^i_{62}\ldots k^i_0$ consists of the 64 leftmost bits of the current contents of register K. Thus at round i, K_i is as follows:

$$K_i = k^i_{63}k^i_{62}\ldots k^i_0 = k_{127}k_{126}\ldots k_{64}$$

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

1) $k_{127}k_{126}...k_1k_0 \leftarrow k_{66}k_{65}...k_{68}k_{67}$

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) $k_{66}k_{65}k_{64}k_{63}k_{62} \leftarrow k_{66}k_{65}k_{64}k_{63}k_{62} \oplus round_counter$

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 $k_{66}k_{65}k_{64}k_{63}k_{62}$

© ISO/IEC 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29192-2:2019

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

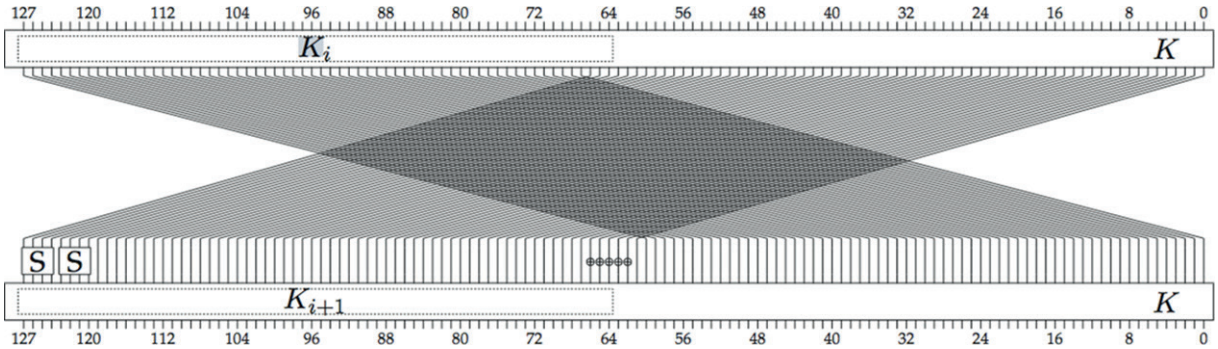

Figure 5 — PRESENT-128 key schedule

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[15] 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)
$<<<i$	i-bit left cyclic shift operation
$\sim a$	bitwise complement of bit string a
Σ^n	n times operations of the DoubleSwap function Σ

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, $C_i \in \{0,1\}^{32}$ $(0 \le i < 4)$ be divided plaintexts

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29192-2:2019

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

ENC_r:

1) $T_0 \| T_1 \| T_2 \| T_3 \leftarrow P_0 \| (P_1 \oplus WK_0) \| P_2 \| (P_3 \oplus WK_1)$

2) $T_0 \| T_1 \| T_2 \| T_3 \leftarrow GFN_{4,r}(RK_0, \ldots, RK_{2r-1}, T_0, T_1, T_2, T_3)$

3) $C_0 \| C_1 \| C_2 \| C_3 \leftarrow T_0 \| (T_1 \oplus WK_2) \| T_2 \| (T_3 \oplus WK_3)$

6.2.4 CLEFIA decryption

The decryption function DEC_r is defined as follows:

DEC_r:

1) $T_0 \| T_1 \| T_2 \| T_3 \leftarrow C_0 \| (C_1 \oplus WK_2) \| C_2 \| (C_3 \oplus WK_3)$

2) $T_0 \| T_1 \| T_2 \| T_3 \leftarrow GFN_{4,r}^{-1}(RK_0, \ldots, RK_{2r-1}, T_0, T_1, T_2, T_3)$

3) $P_0 \| P_1 \| P_2 \| P_3 \leftarrow T_0 \| (T_1 \oplus WK_0) \| T_2 \| (T_3 \oplus WK_1)$

Figure 6 illustrates both ENC_r and DEC_r.

© ISO/IEC 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29192-2:2019

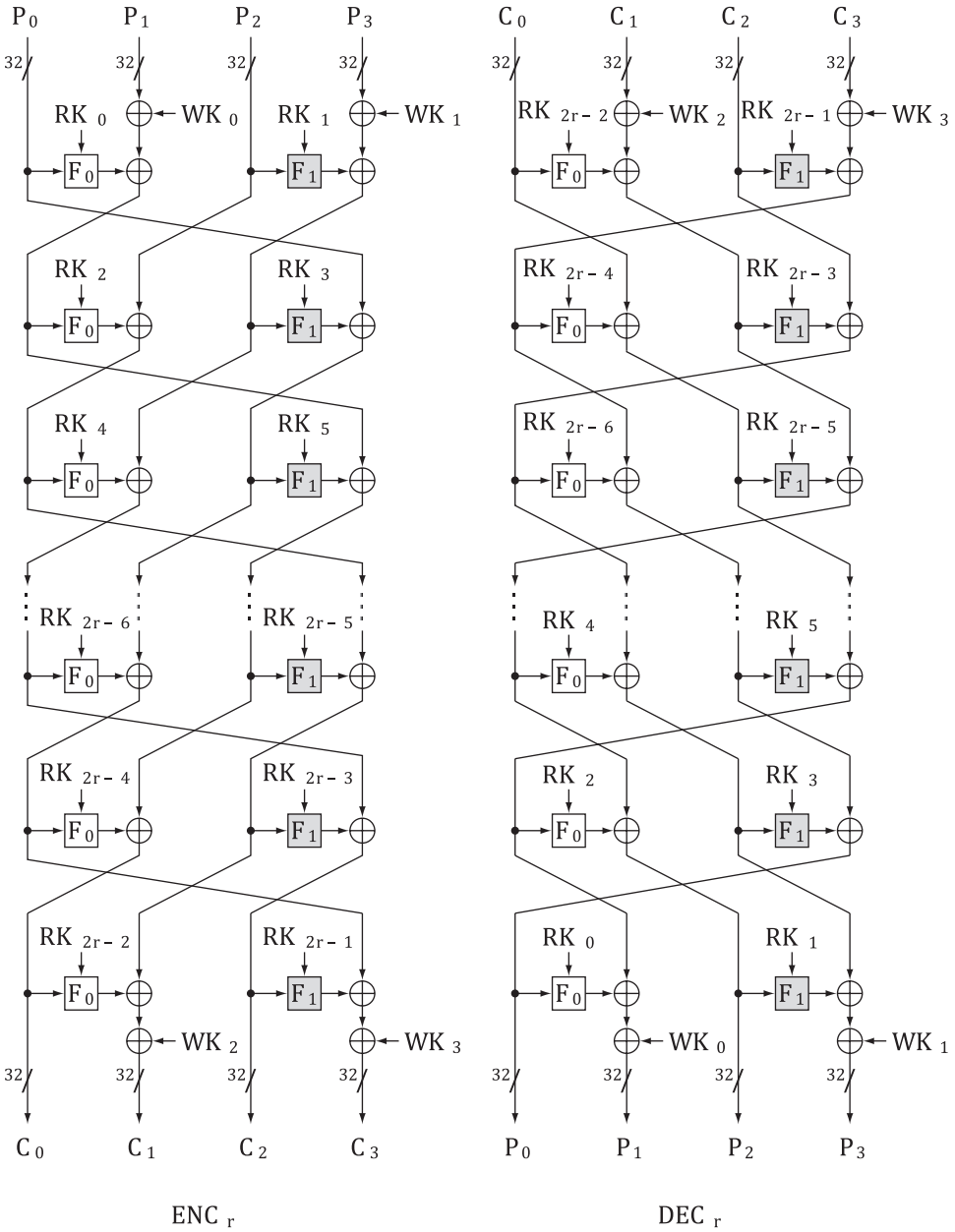

Figure 6 — The encryption procedure and the decryption procedure of CLEFIA

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

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29192-2:2019

$GFN_{4,r}$:

1) $T_0 \| T_1 \| T_2 \| T_3 \leftarrow X_0 \| X_1 \| X_2 \| X_3$

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) $T_0 \| T_1 \| T_2 \| T_3 \leftarrow T_1 \| T_2 \| T_3 \| T_0$

3) $Y_0 \| Y_1 \| Y_2 \| Y_3 \leftarrow T_3 \| T_0 \| T_1 \| T_2$

$GFN_{8,r}$:

1) $T_0 \| T_1 \| \ldots \| T_7 \leftarrow X_0 \| X_1 \| \ldots \| X_7$

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) $T_0 \| T_1 \| \ldots \| T_6 \| T_7 \leftarrow T_1 \| T_2 \| \ldots \| T_7 \| T_0$

3) $Y_0 \| Y_1 \| \ldots \| Y_6 \| Y_7 \leftarrow T_7 \| T_0 \| \ldots \| T_5 \| T_6$

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) $T_0 \| T_1 \| T_2 \| T_3 \leftarrow X_0 \| X_1 \| X_2 \| X_3$

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) $T_0 \| T_1 \| T_2 \| T_3 \leftarrow T_3 \| T_0 \| T_1 \| T_2$

3) $Y_0 \| Y_1 \| Y_2 \| Y_3 \leftarrow T_1 \| T_2 \| T_3 \| T_0$

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 $V = V_0 \| V_1 \| V_2 \| V_3$, $V_i \in \{0,1\}^8$.

   $V_0 \leftarrow S_0(V_0)$

   $V_1 \leftarrow S_1(V_1)$

© ISO/IEC 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29192-2:2019

$V_2 \leftarrow S_0(V_2)$

$V_3 \leftarrow S_1(V_3)$

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 × 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.

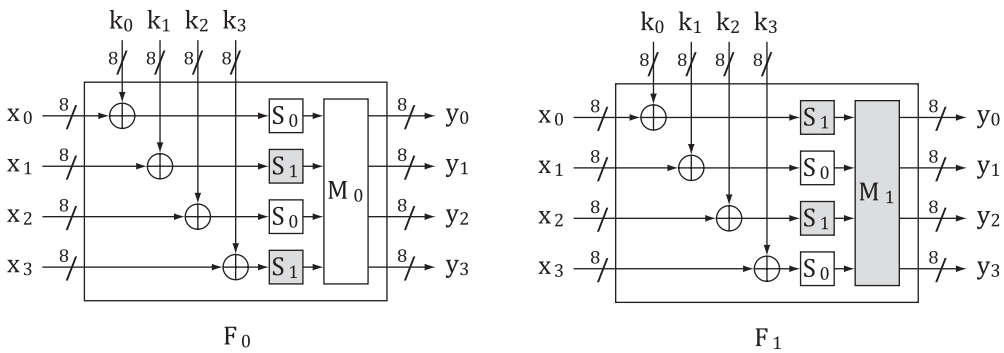

Figure 7 — F-functions

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

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29192-2:2019

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 $x = x_0 \| x_1, x_i \in \{0,1\}^4$

2) $u_0 \leftarrow t_0 \oplus \texttt{0x2} \cdot t_1, u_1 \leftarrow \texttt{0x2} \cdot t_0 \oplus t_1$

3) $y_0 \leftarrow SS_2(u_0), y_1 \leftarrow SS_3(u_1)$, where $y = y_0 \| y_1, y_i \in \{0,1\}^4$

© ISO/IEC 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 29192-2:2019