別添３

○総務省告示第百六十九号

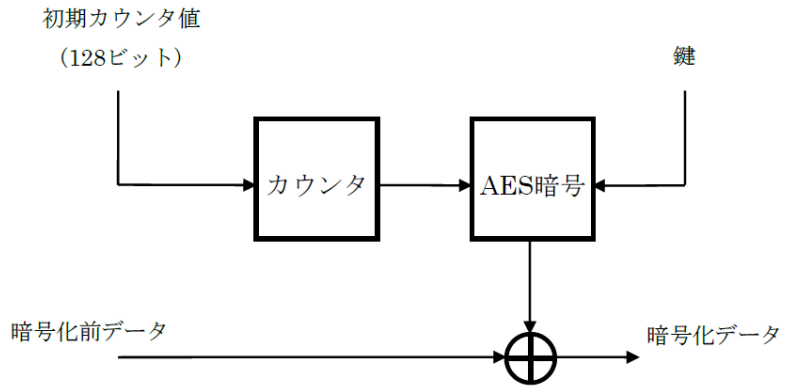
標準テレビジョン放送等のうちデジタル放送に関する送信の標準方式（平成二十三年総務省令第八十七号）第二十三条の十九（第二十三条の二十四において準用する場合を含む。）及び第六十五条の二（第二十四条において準用する場合を含む。）の規定に基づき、平成二十六年総務省告示第二百三十五号（スクランブルの方式を定める件）の一部を次のように改正する。

令和六年五月二十三日

総務大臣　松本　剛明

次の表により、改正後欄に掲げるその標記部分に二重傍線（二重下線を含む。）を付した規定（以下「対象規定」という。）は、これを加える。

改　正　後	改　正　前
［１・２　略］	［１・２　同上］
２の２　標準方式第二十三条の十九の規定に基づくスクランブルの方式は次の各号に掲げるとおりとする。	［新設］
一　スクランブルの範囲は、ＭＭＴＰパケットにあってはＭＭＴＰパケットのペイロード部のうちデータ部（全部又はその一部）とし、ＩＰパケットにあってはペイロード部とする。	
二　スクランブルの手順は、別表第三号の二から別表第三号の五までのいずれかのとおりとする。	
［３　略］	［３　同上］
４　標準方式第六十五条の二の規定に基づくスクランブルの方式は次の各号に掲げるとおりとする。	［４　同上］
［一・二　略］	［一・二　同上］
三　標準方式第三章の三第二節に定める放送のスクランブルの範囲及びスクランブルの手順は、第一号及び前号の規定にかかわらず、第二項の二第一号及び第二号のとおりとする。	［新設］
別表第三号の二	［新設］



注１　鍵長は128ビット、192ビット又は256ビットとする。

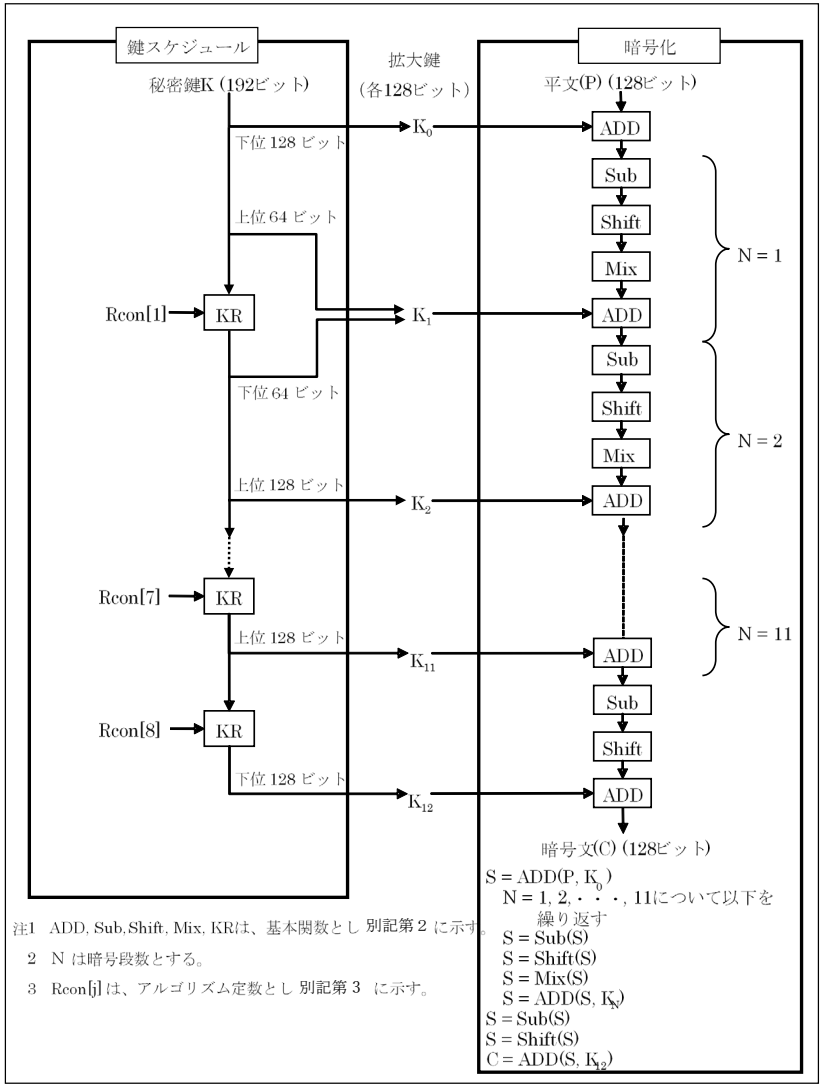
２　ＡＥＳ暗号は、別記第１に示す。

別記第１　ＡＥＳ暗号

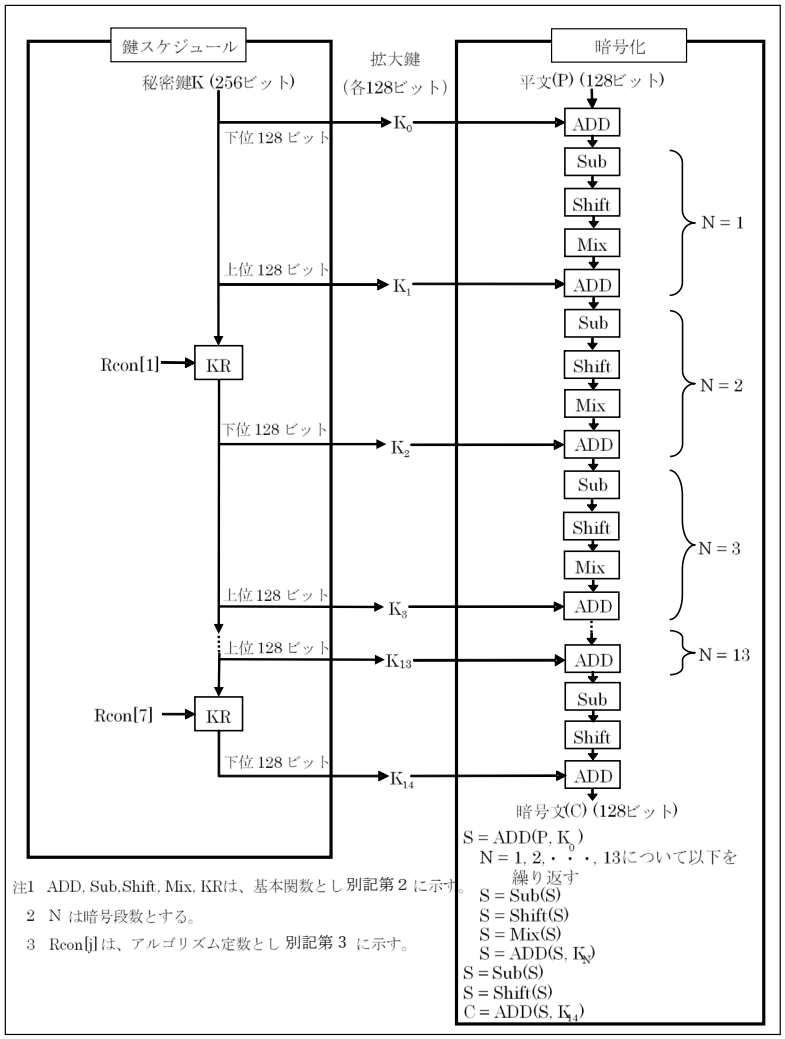
⑴　鍵長が128ビットの場合

別表第二号別記第１に示すとおりとする。

⑵　鍵長が192ビットの場合

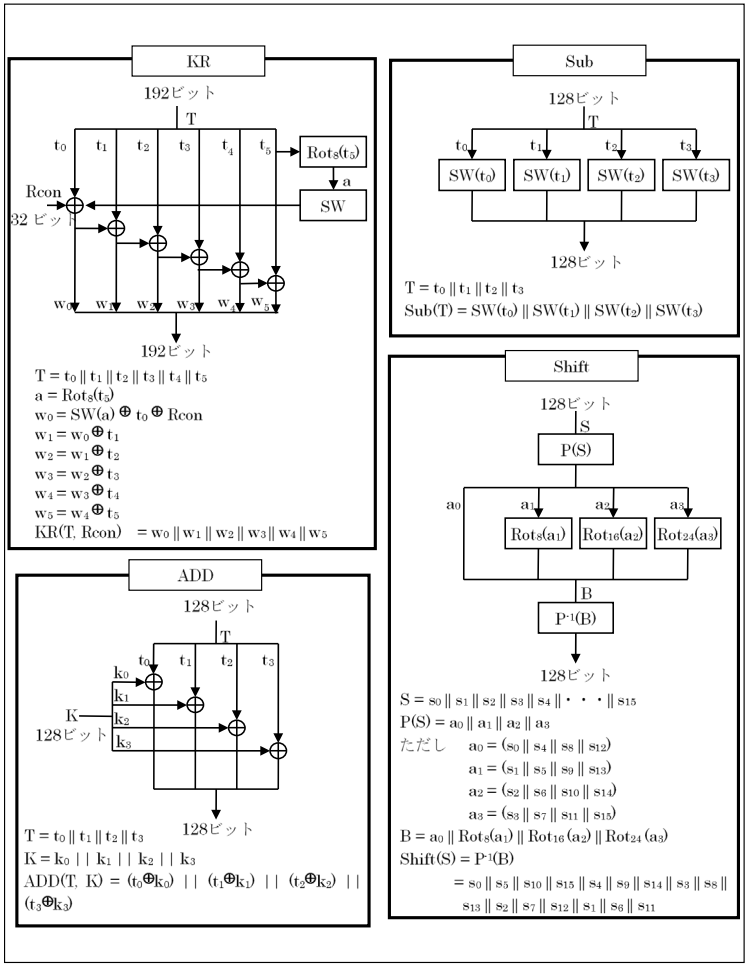


(3) 鍵長が256ビットの場合

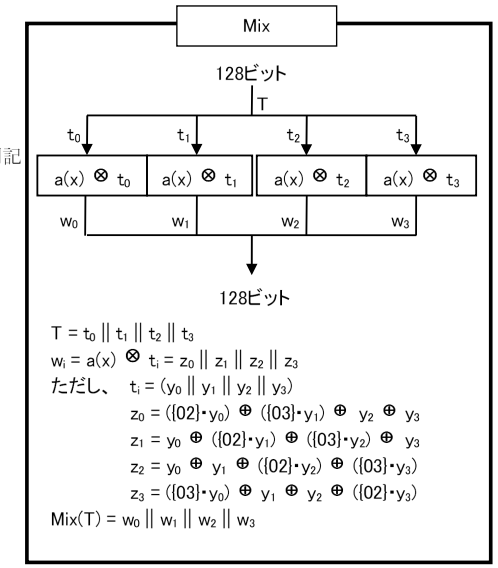


別記第２　基本関数

⑴　鍵長が192ビットの場合

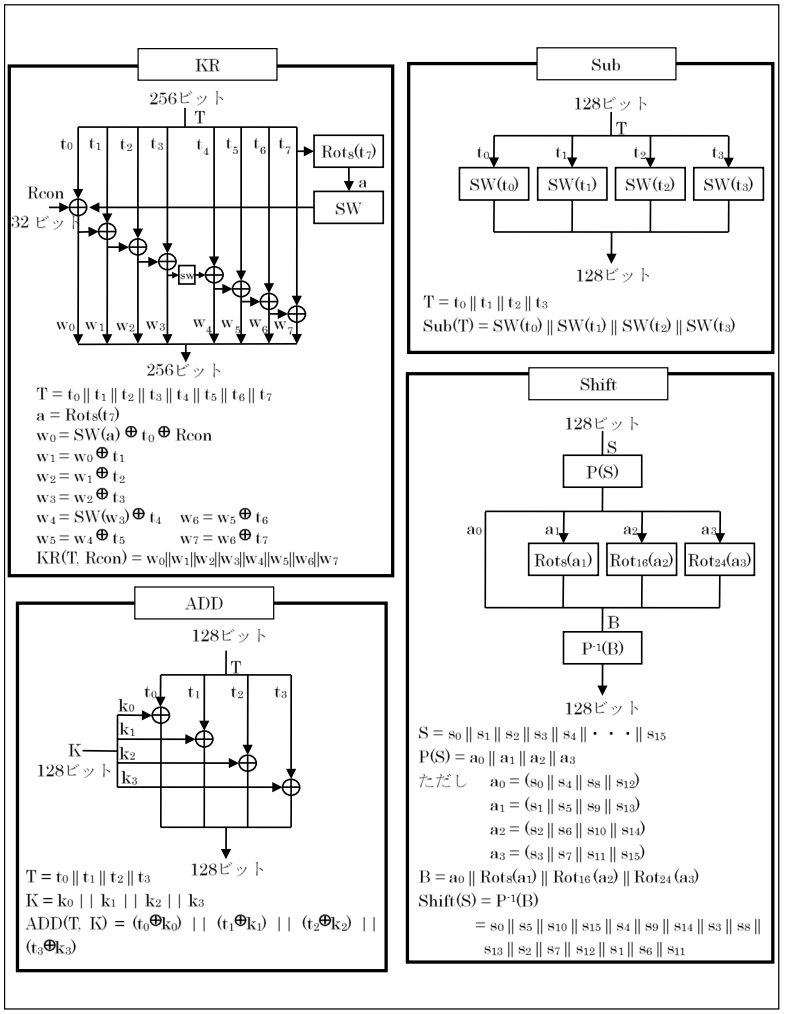

KR
192ビット
T
t0 t1 t2 t3 t4 t5
Rot8(t5)
a
SW
Rcon
32 ビット
w0 w1 w2 w3 w4 w5
192ビット
T = t0 || t1 || t2 || t3 || t4 || t5
a = Rot8(t5)
w0 = SW(a) ⊕ t0 ⊕ Rcon
w1 = w0 ⊕ t1
w2 = w1 ⊕ t2
w3 = w2 ⊕ t3
w4 = w3 ⊕ t4
w5 = w4 ⊕ t5
KR(T, Rcon) = w0 || w1 || w2 || w3 || w4 || w5
Sub
128ビット
T
t0 t1 t2 t3
SW(t0) SW(t1) SW(t2) SW(t3)
128ビット
T = t0 || t1 || t2 || t3
Sub(T) = SW(t0) || SW(t1) || SW(t2) || SW(t3)
Shift
128ビット
S
P(S)
a0 a1 a2 a3
Rot8(a1) Rot16(a2) Rot24(a3)
B
P-1(B)
128ビット
S = s0 || s1 || s2 || s3 || s4 || ・・・ || s15
P(S) = a0 || a1 || a2 || a3
ただし a0 = (s0 || s4 || s8 || s12)
a1 = (s1 || s5 || s9 || s13)
a2 = (s2 || s6 || s10 || s14)
a3 = (s3 || s7 || s11 || s15)
B = a0 || Rot8(a1) || Rot16(a2) || Rot24(a3)
Shift(S) = P-1(B)
= s0 || s5 || s10 || s15 || s4 || s9 || s14 || s3 || s8 ||
s13 || s2 || s7 || s12 || s1 || s6 || s11
ADD
128ビット
T
t0 t1 t2 t3
k0 k1 k2 k3
K
128ビット
128ビット
T = t0 || t1 || t2 || t3
K = k0 || k1 || k2 || k3
ADD(T, K) = (t0⊕k0) || (t1⊕k1) || (t2⊕k2) ||
(t3⊕k3)

注1　Tは、基本関数への入力とする。
2　⊕は、ビット毎の排他的論理和とする。
3　‖ は、ブロックの結合とする。
4　SWは、補助関数とし別表第二号別記第４に示す。
5　Rot_n は、左巡回nビットシフトとする。
6　・は、GF(2^8)上の乗算を表す。
既約多項式は、
$x^8 + x^4 + x^3 + x + 1$とする。

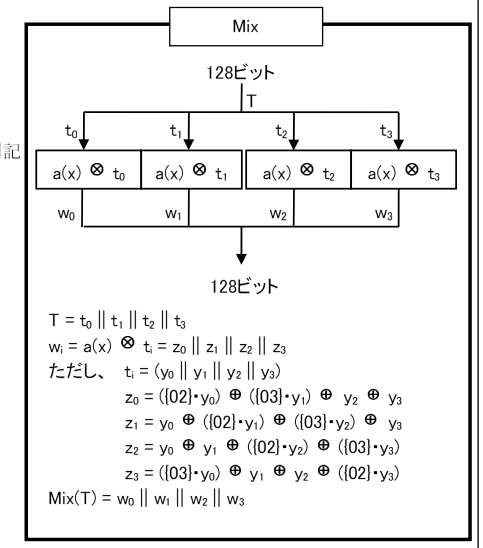


$T = t_0 \| t_1 \| t_2 \| t_3$
$w_i = a(x) \otimes t_i = z_0 \| z_1 \| z_2 \| z_3$
ただし、 $t_i = (y_0 \| y_1 \| y_2 \| y_3)$
$z_0 = ([02]\cdot y_0) \oplus ([03]\cdot y_1) \oplus y_2 \oplus y_3$
$z_1 = y_0 \oplus ([02]\cdot y_1) \oplus ([03]\cdot y_2) \oplus y_3$
$z_2 = y_0 \oplus y_1 \oplus ([02]\cdot y_2) \oplus ([03]\cdot y_3)$
$z_3 = ([03]\cdot y_0) \oplus y_1 \oplus y_2 \oplus ([02]\cdot y_3)$
$Mix(T) = w_0 \| w_1 \| w_2 \| w_3$

(2)　鍵長が256ビットの場合


KR
256ビット
T
t0 t1 t2 t3 t4 t5 t6 t7
Rot8(t7)
a
SW
Rcon
32 ビット
sw
w0 w1 w2 w3 w4 w5 w6 w7
256ビット
T = t0 || t1 || t2 || t3 || t4 || t5 || t6 || t7
a = Rot8(t7)
w0 = SW(a) ⊕ t0 ⊕ Rcon
w1 = w0 ⊕ t1
w2 = w1 ⊕ t2
w3 = w2 ⊕ t3
w4 = SW(w3) ⊕ t4 w6 = w5 ⊕ t6
w5 = w4 ⊕ t5 w7 = w6 ⊕ t7
KR(T, Rcon) = w0||w1||w2||w3||w4||w5||w6||w7
Sub
128ビット
T
t0 t1 t2 t3
SW(t0) SW(t1) SW(t2) SW(t3)
128ビット
T = t0 || t1 || t2 || t3
Sub(T) = SW(t0) || SW(t1) || SW(t2) || SW(t3)
Shift
128ビット
S
P(S)
a0 a1 a2 a3
Rot8(a1) Rot16(a2) Rot24(a3)
B
P-1(B)
128ビット
S = s0 || s1 || s2 || s3 || s4 || ・・・|| s15
P(S) = a0 || a1 || a2 || a3
ただし a0 = (s0 || s4 || s8 || s12)
a1 = (s1 || s5 || s9 || s13)
a2 = (s2 || s6 || s10 || s14)
a3 = (s3 || s7 || s11 || s15)
B = a0 || Rot8(a1) || Rot16(a2) || Rot24(a3)
Shift(S) = P-1(B)
= s0 || s5 || s10 || s15 || s4 || s9 || s14 || s3 || s8 ||
s13 || s2 || s7 || s12 || s1 || s6 || s11
ADD
128ビット
T
t0 t1 t2 t3
k0 k1 k2 k3
K
128ビット
128ビット
T = t0 || t1 || t2 || t3
K = k0 || k1 || k2 || k3
ADD(T, K) = (t0⊕k0) || (t1⊕k1) || (t2⊕k2) || (t3⊕k3)

注1　Tは、基本関数への入力とする。
2　⊕は、ビット毎の排他的論理和とする。
3　‖ は、ブロックの結合とする。
4　SWは、補助関数とし別表第二号別記第４に示す。
5　Rot_n は、左巡回nビットシフトとする。
6　・は、GF(2^8)上の乗算を表す。
既約多項式は、
$x^8 + x^4 + x^3 + x + 1$とする。

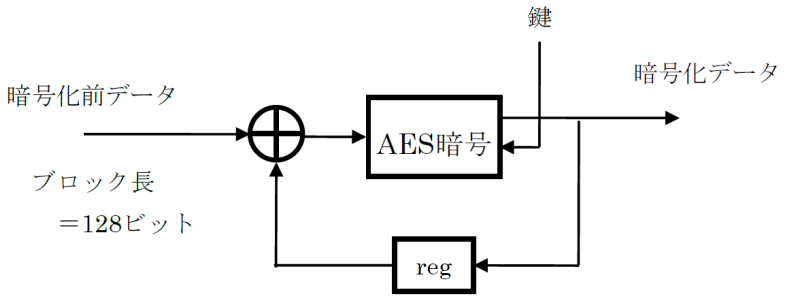


$T = t_0 \| t_1 \| t_2 \| t_3$
$w_i = a(x) \otimes t_i = z_0 \| z_1 \| z_2 \| z_3$
ただし、 $t_i = (y_0 \| y_1 \| y_2 \| y_3)$
$z_0 = ([02]\cdot y_0) \oplus ([03]\cdot y_1) \oplus y_2 \oplus y_3$
$z_1 = y_0 \oplus ([02]\cdot y_1) \oplus ([03]\cdot y_2) \oplus y_3$
$z_2 = y_0 \oplus y_1 \oplus ([02]\cdot y_2) \oplus ([03]\cdot y_3)$
$z_3 = ([03]\cdot y_0) \oplus y_1 \oplus y_2 \oplus ([02]\cdot y_3)$
$Mix(T) = w_0 \| w_1 \| w_2 \| w_3$

別記第３　アルゴリズム定数
⑴　鍵長が192ビットの場合
Rcon[１]＝01000000
Rcon[２]＝02000000
Rcon[３]＝04000000
Rcon[４]＝08000000
Rcon[５]＝10000000
Rcon[６]＝20000000
Rcon[７]＝40000000
Rcon[８]＝80000000
注　数値は16進数表記とする。
⑵　鍵長が256ビットの場合
Rcon[１]＝01000000
Rcon[２]＝02000000
Rcon[３]＝04000000
Rcon[４]＝08000000
Rcon[５]＝10000000

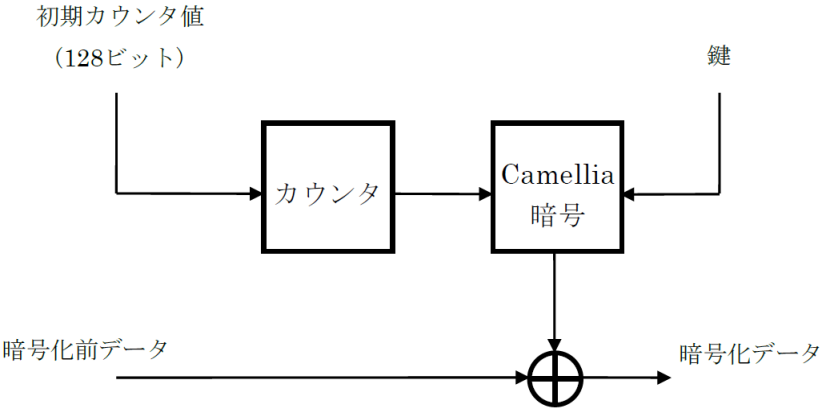
Rcon[６]＝20000000
Rcon[７]＝40000000
注　数値は16進数表記とする。

別表第三号の三



注１　ブロック長が128ビットに満たないブロックは暗号化しないこととする。
２　鍵長は128ビット、192ビット又は256ビットとする。
３　ＡＥＳ暗号は、別表第三号の二別記第１に示す。

別表第三号の四



注１　鍵長は128ビット、192ビット又は256ビットとする。
２　Camellia暗号は、別記第１に示す。

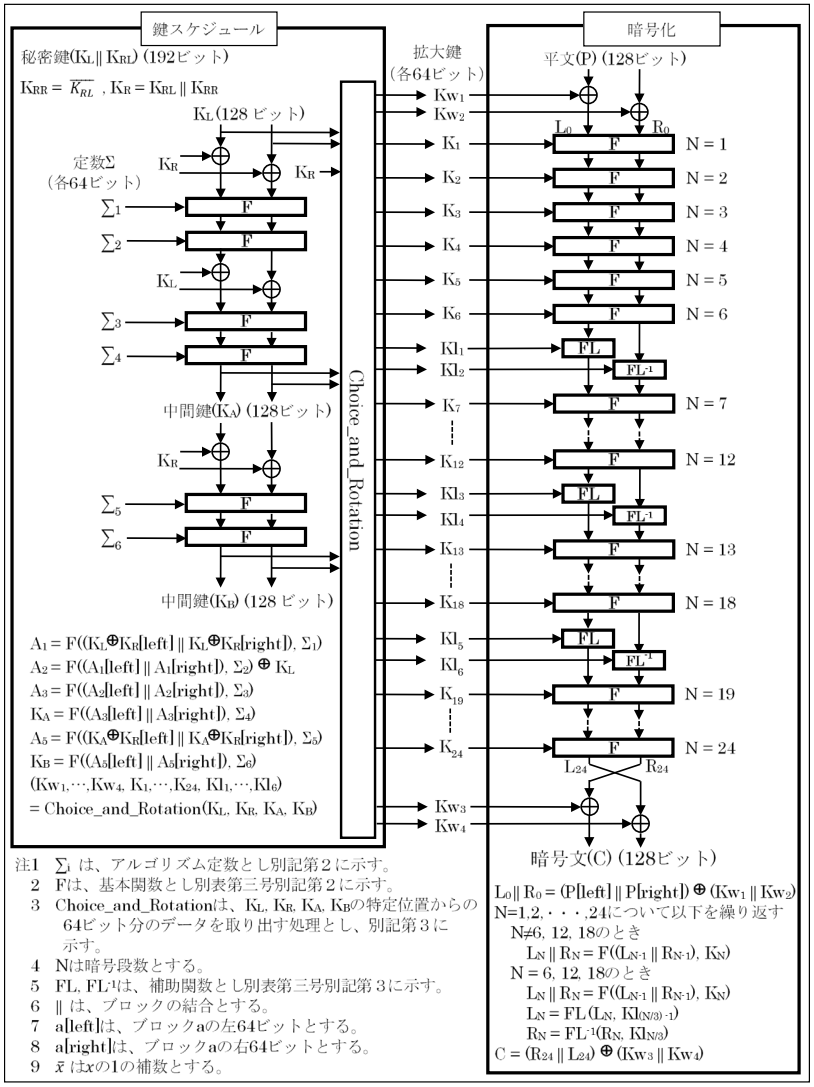
別記第１　Camellia暗号

⑴　鍵長が128ビットの場合
別表第三号別記第１に示す。

⑵　鍵長が192ビットの場合

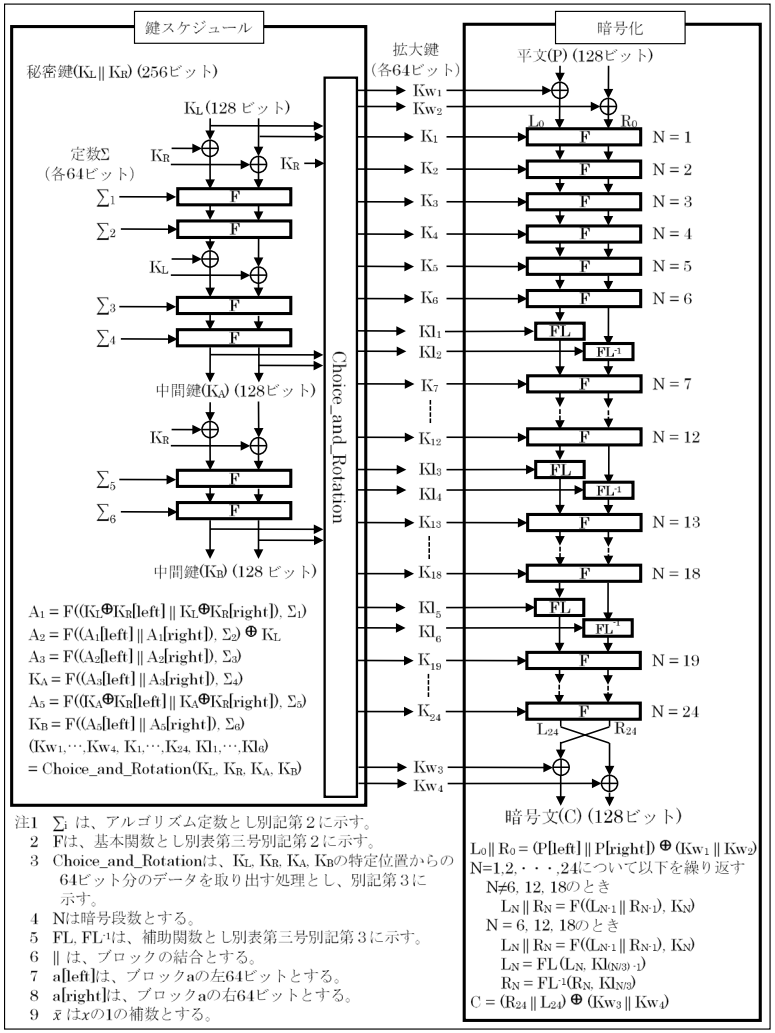
［新設］

［新設］



注1　$\sum_i$ は、アルゴリズム定数とし別記第２に示す。
2　Fは、基本関数とし別表第三号別記第２に示す。
3　Choice_and_Rotationは、KL, KR, KA, KBの特定位置からの64ビット分のデータを取り出す処理とし、別記第３に示す。
4　Nは暗号段数とする。
5　FL, FL-1は、補助関数とし別表第三号別記第３に示す。
6　‖ は、ブロックの結合とする。
7　a[left]は、ブロックaの左64ビットとする。
8　a[right]は、ブロックaの右64ビットとする。
9　$\bar{x}$ はxの1の補数とする。

⑶　鍵長256ビットの場合



注1　Σ_i は、アルゴリズム定数とし別記第２に示す。
2　Fは、基本関数とし別表第三号別記第２に示す。
3　Choice_and_Rotationは、KL, KR, KA, KBの特定位置からの64ビット分のデータを取り出す処理とし、別記第３に示す。
4　Nは暗号段数とする。
5　FL, FL-1は、補助関数とし別表第三号別記第３に示す。
6　‖ は、ブロックの結合とする。
7　a[left]は、ブロックaの左64ビットとする。
8　a[right]は、ブロックaの右64ビットとする。
9　$\bar{x}$ はxの1の補数とする。

別記第２　アルゴリズム定数

Σ_1＝a09e667f3bcc908b

Σ_2＝b67ae8584caa73b2

Σ_3＝c6ef372fe94f82be

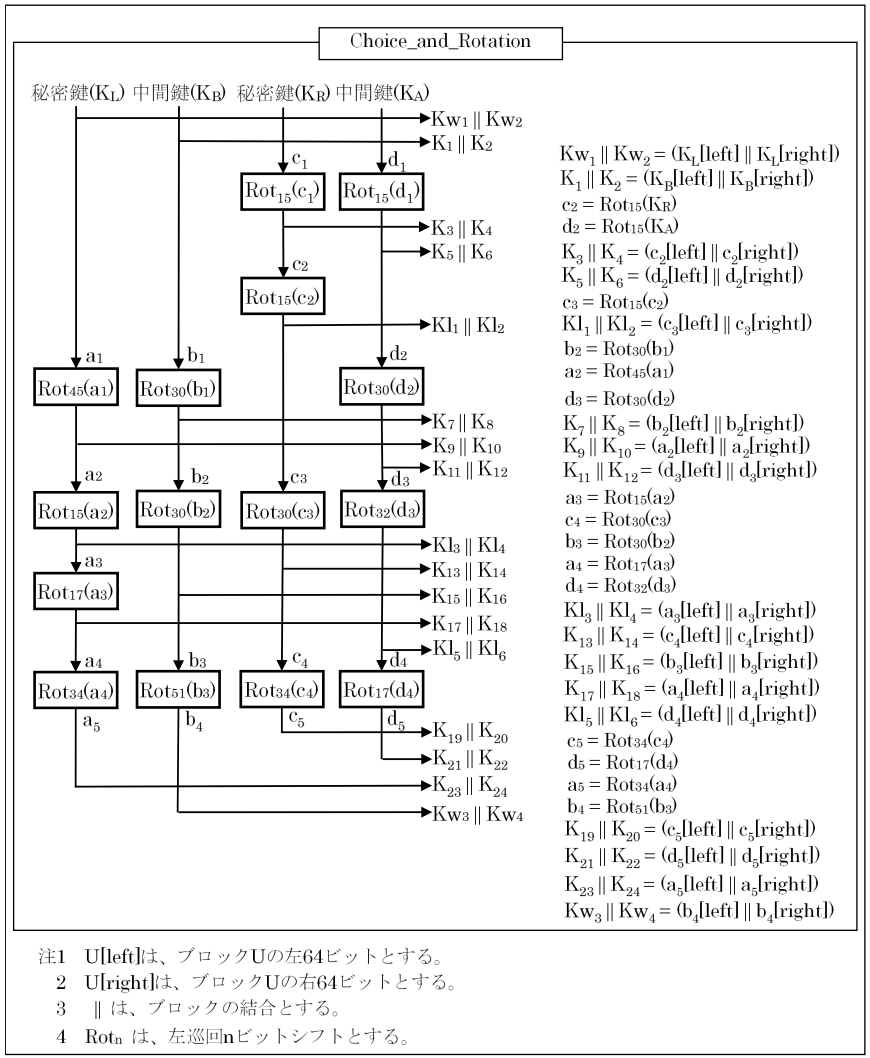
Σ_4＝54ff53a5f1d36f1c

Σ_5＝10e527fade682d1d

Σ_6＝b05688c2b3e6c1fd

注　数値は16進数表記とする。

別記第３　Choice_and_Rotation

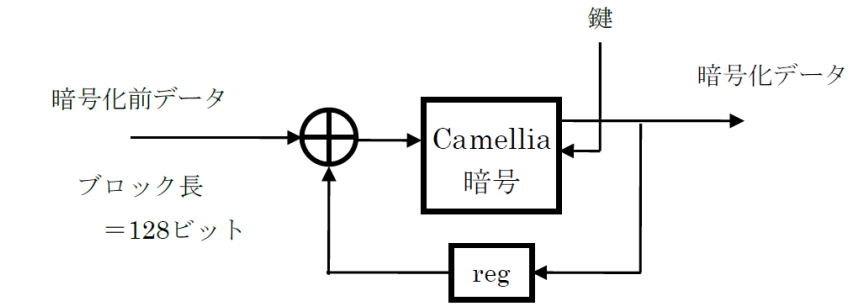


注1　U[left]は、ブロックUの左64ビットとする。

2　U[right]は、ブロックUの右64ビットとする。

3　|| は、ブロックの結合とする。

4　Rotn は、左巡回nビットシフトとする。

別表第三号の五  注１　ブロック長が128ビットに満たないブロックは暗号化しないこととする。 ２　鍵長は128ビット、192ビット又は256ビットとする。 ３　Camellia暗号は、別表第三号の四別記第１に示す。	［新設］
備考　表中の［　］の記載及び対象規定の二重傍線を付した標記部分を除く全体に付した傍線は注記である。	