○総務省告示第二百三十五号

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）第八条第一号及び第二号、第四十七条並びに第六十五条の二の規定に基づき、スクランブルの方式を次のように定め、平成二十六年七月三日から施行する。

なお、平成二十三年総務省告示第三百二号（スクランブルの方式を定める件）は、平成二十六年七月三日限り廃止する。

平成二十六年七月三日

総務大臣臨時代理
国務大臣　田村　憲久

1　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。以下「標準方式」という。）第八条第一号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。

一　スクランブルの範囲は、ＴＳパケット（伝送制御信号及び関連情報を送るためのものを除く。）のペイロード部とする。

二　スクランブルの手順は、別表第一号のとおりとする。

三　標準方式第四章第一節及び第二節、第五章第二節並びに第六章第三節に定める放送のスクラン

ブルの手順は、前号の規定にかかわらず、別表第一号から別表第三号までのいずれかのとおりとする。

四　標準方式第五章第三節及び第六章第五節に定める放送のスクランブルの手順は、第二号に定める規定にかかわらず、別表第二号又は別表第三号のいずれかのとおりとする。

2　標準方式第八条第二号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。

一　スクランブルの範囲は、平成二十三年総務省告示第三百一号（映像信号のうちセクション形式によるもの及び音声信号のうちセクション形式によるものの送出手順を定める件）第２項に定めるモジュールとする。

二　スクランブルを行ったモジュールには、当該スクランブルの手順を識別する情報、当該スクランブルの解除の手順を識別する情報、当該モジュールを含む放送番組を識別する情報及び当該スクランブルに関する関連情報を識別する情報を含む情報を付加することとする。

3　標準方式第四十七条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。

一　スクランブルの範囲は、同期パケットを伝送するトランスポートフレーム全体とする。

二　スクランブルの手順は、別表第四号から別表第七号までのいずれかのとおりとする。

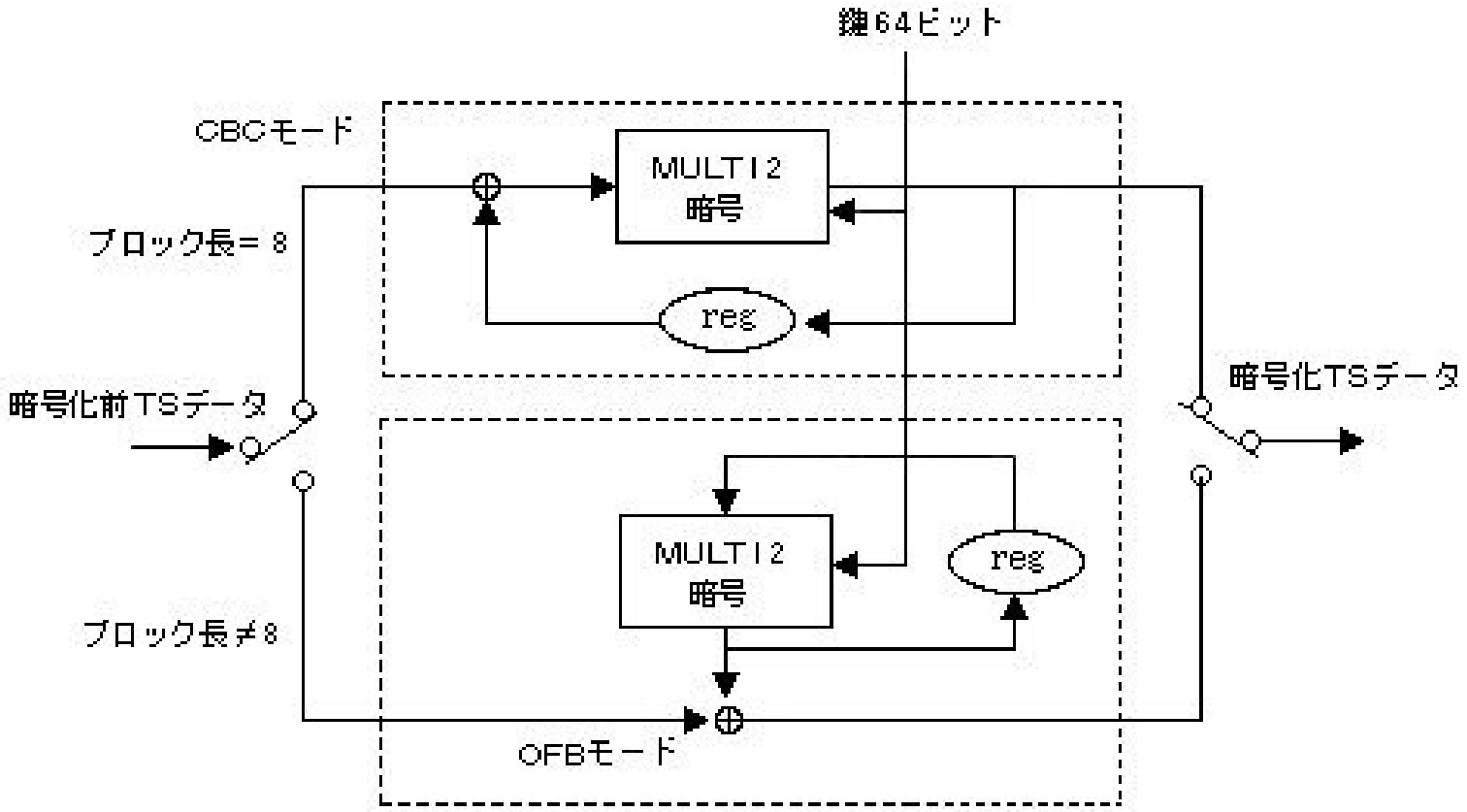
4　標準方式第六十五条の二の規定に基づくスクランブルの方式は次の各号に掲げるとおりとする。

一　スクランブルの範囲は、ＭＭＴＰパケットにあってはペイロード部のうちデータ部とし、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、別表第八号又は別表第九号のいずれかのとおりとする。

別表第一号

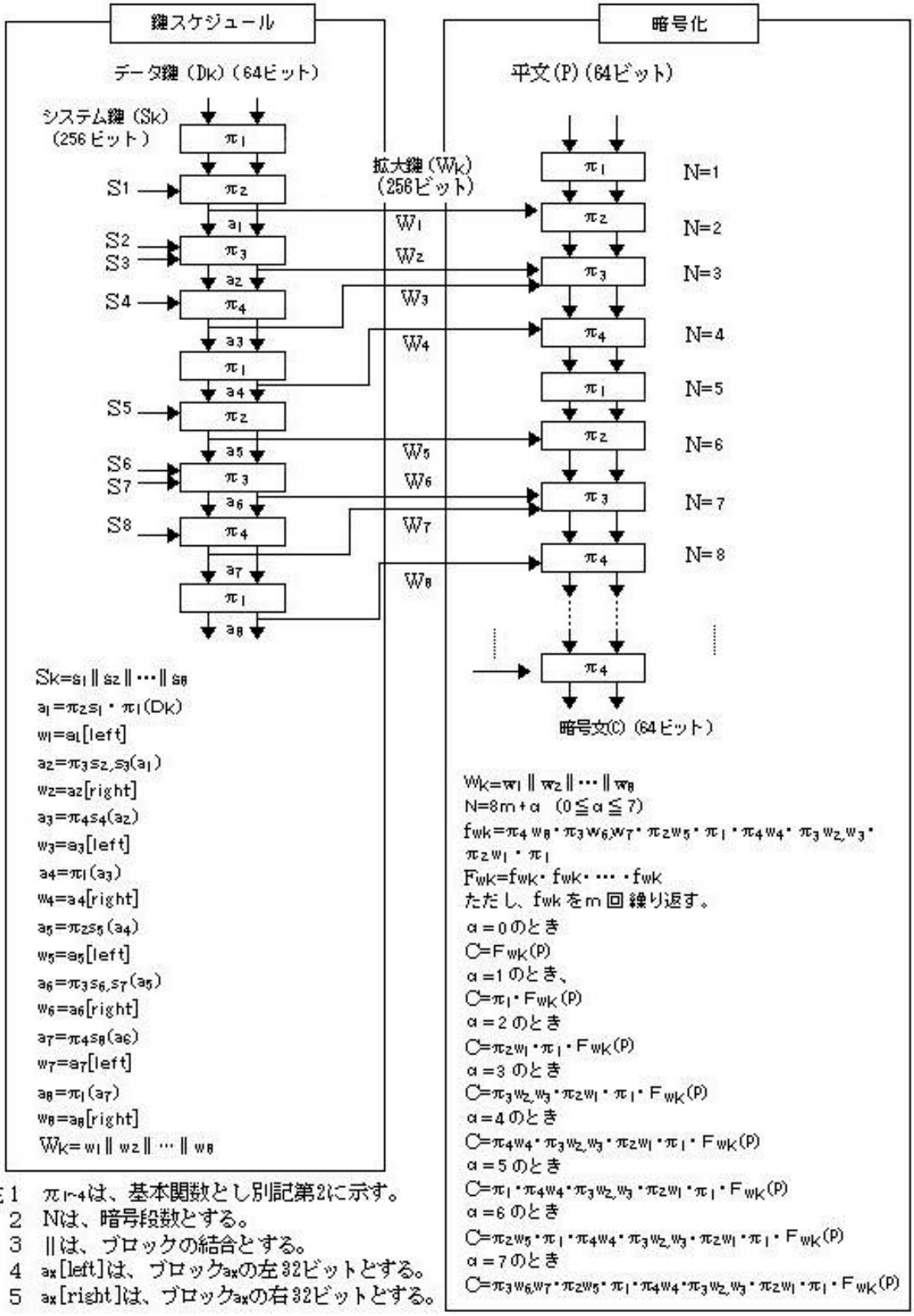


注１　ＭＵＬＴＩ２暗号は、別記第１に示す。

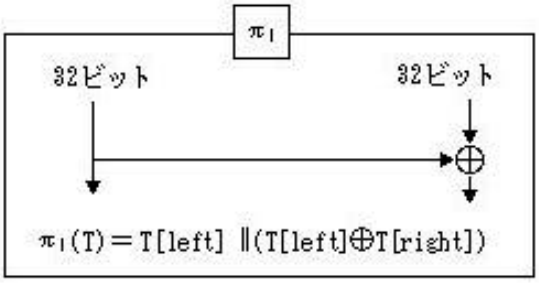
２　reg　は、レジスタを示す。以下同じ。

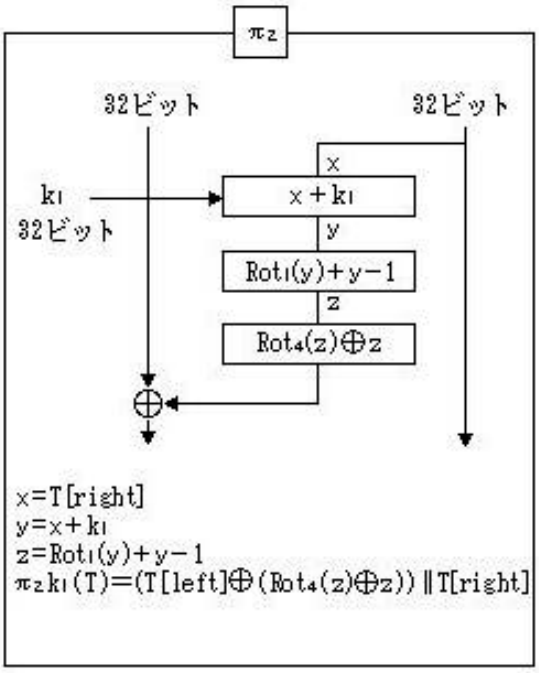
３　⊕は、排他的論理和を示す。以下同じ。

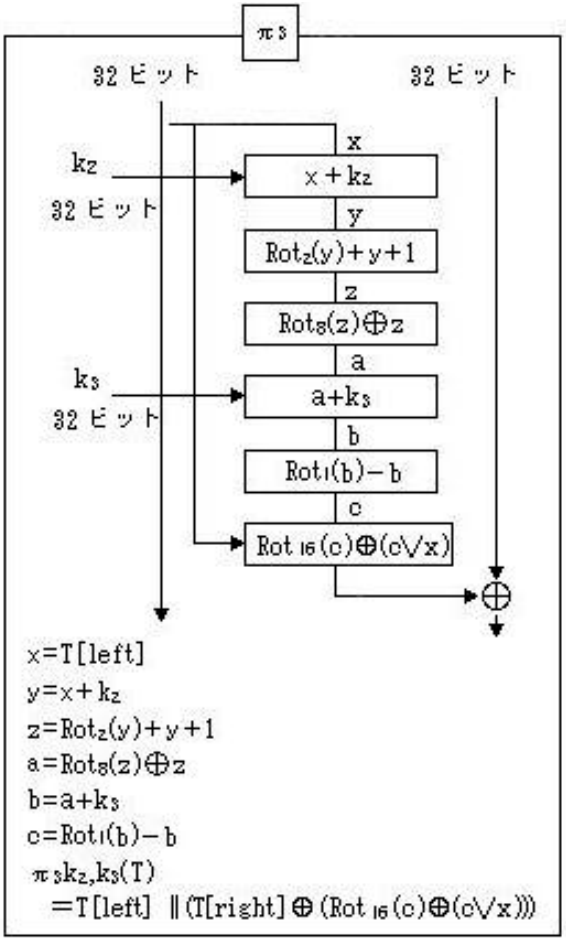
回

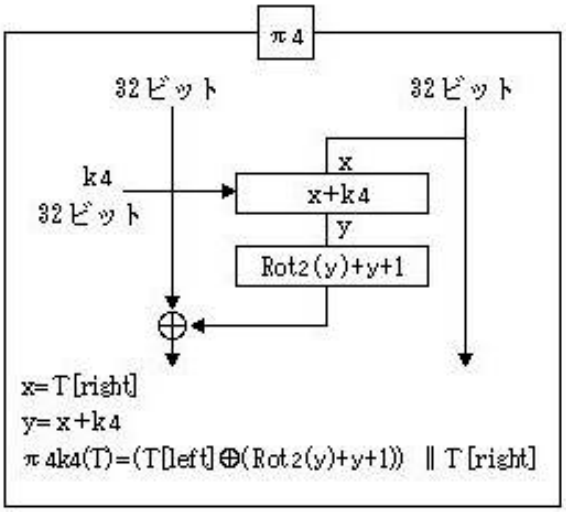


注１　π1~4は、基本関数とし別記第2に示す。
２　Nは、暗号段数とする。
３　‖は、ブロックの結合とする。
４　ax[left]は、ブロックaxの左32ビットとする。
５　ax[right]は、ブロックaxの右32ビットとする。



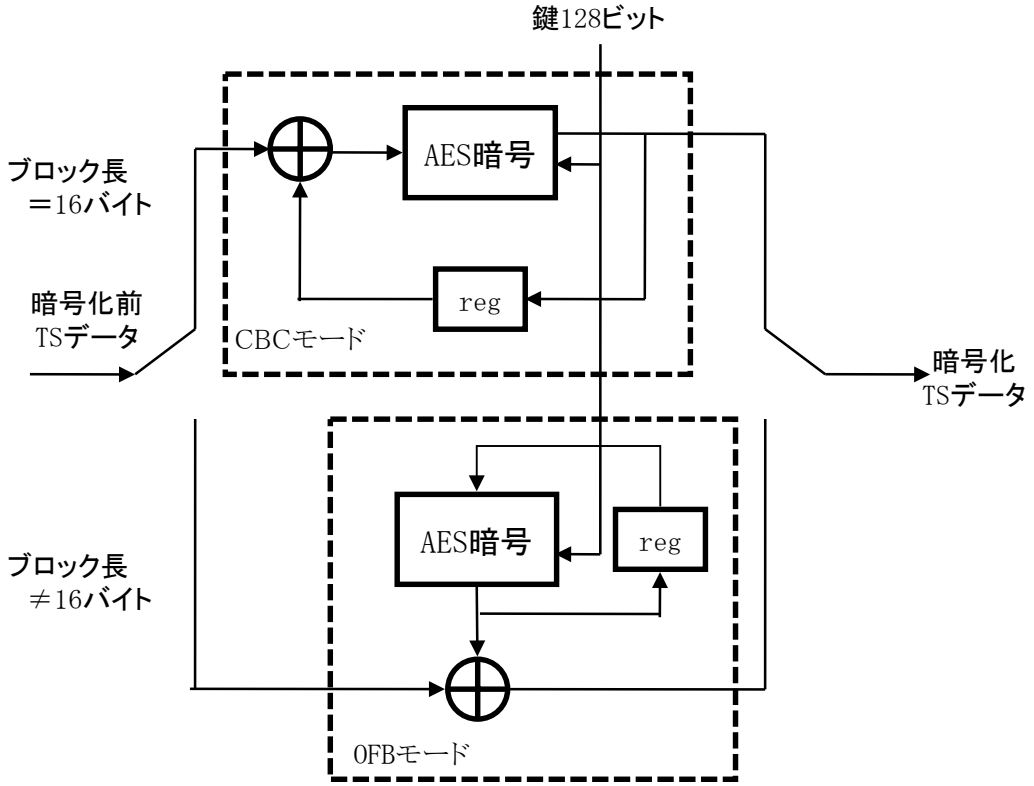






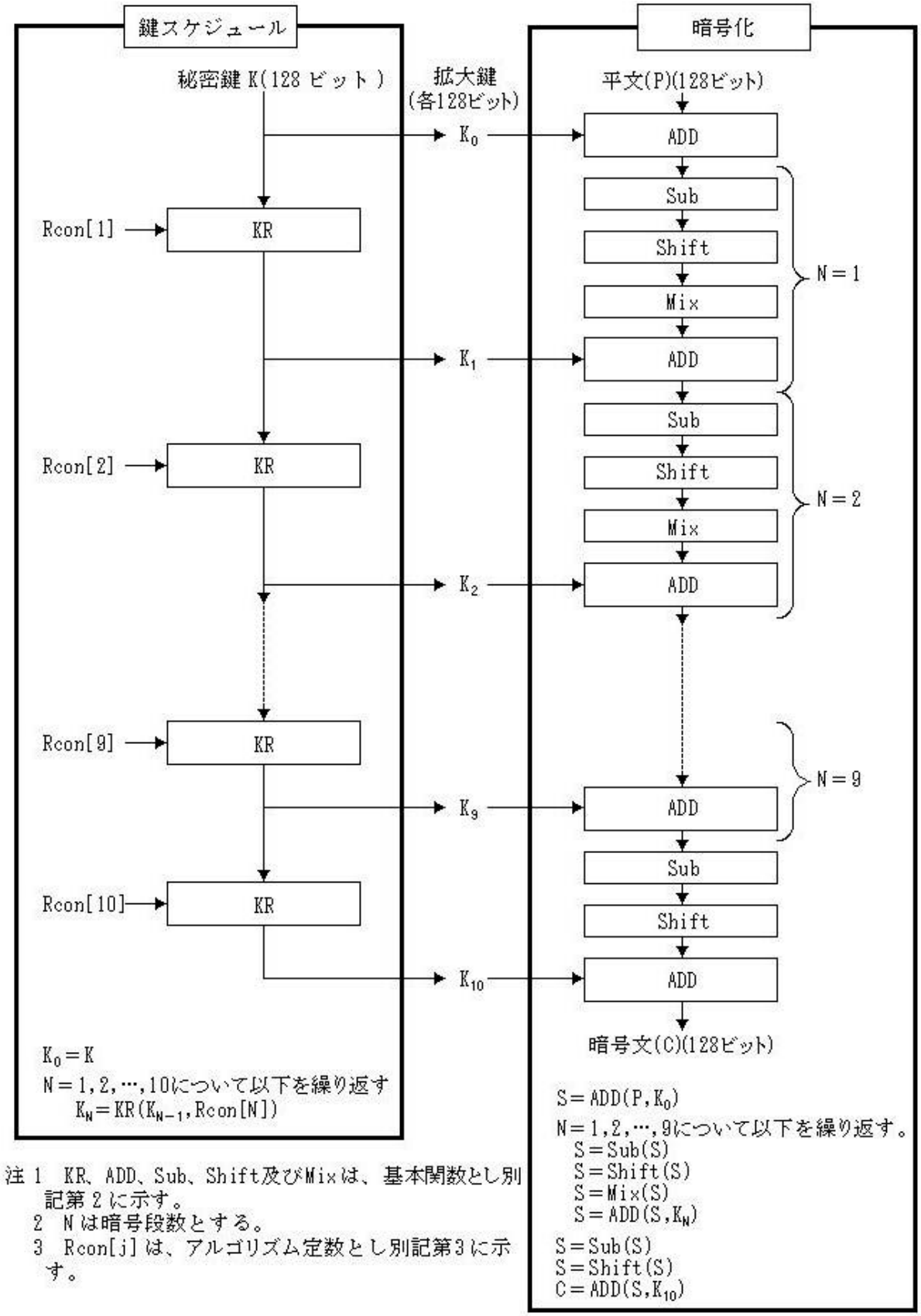
注１　Ｔは、基本関数への入力とする。
　２　Ｔ[left]は、ブロックＴの左32ビットとする。
　３　Ｔ[right]は、ブロックＴの右32ビットとする。
　４　＋は、2^{32}を法とした加算とする。
　５　－は、2^{32}を法とした減算とする。
　６　Rotsは、左巡回ｓビットシフトとする。
　７　∨は、ビット毎の論理和とする。
　８　‖は、ブロックの結合とする。

別表第二号

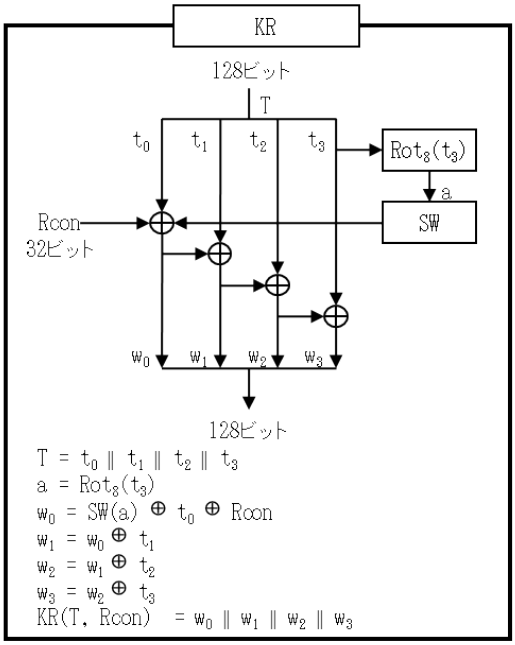


注　ＡＥＳ暗号は、別記第１に示す。

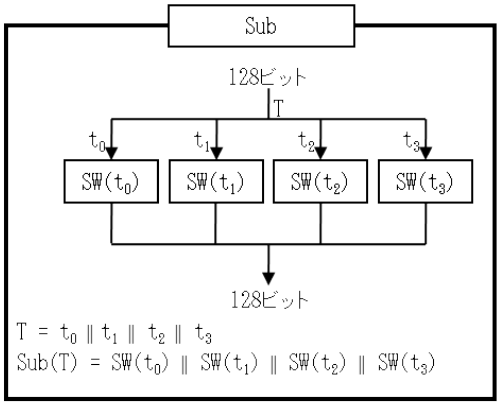
別記第１　ＡＥＳ暗号



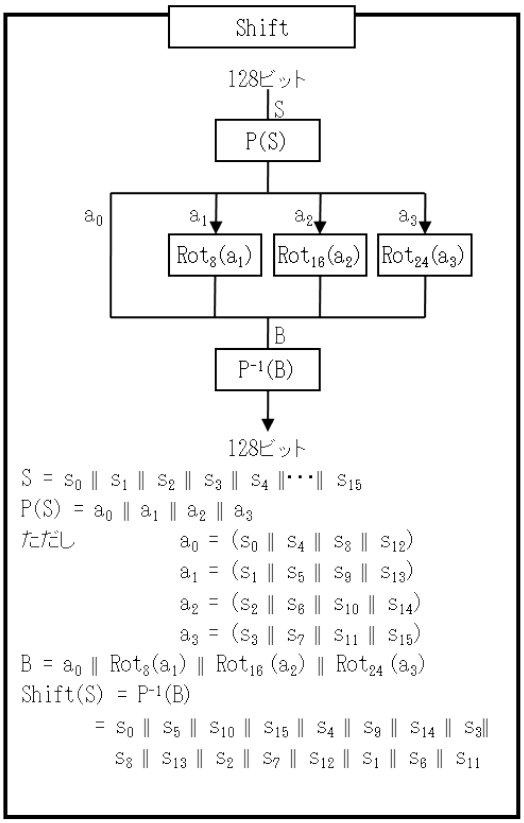
注 1　KR、ADD、Sub、Shift及びMixは、基本関数とし別記第２に示す。
2　Ｎは暗号段数とする。
3　Rcon[j]は、アルゴリズム定数とし別記第３に示す。



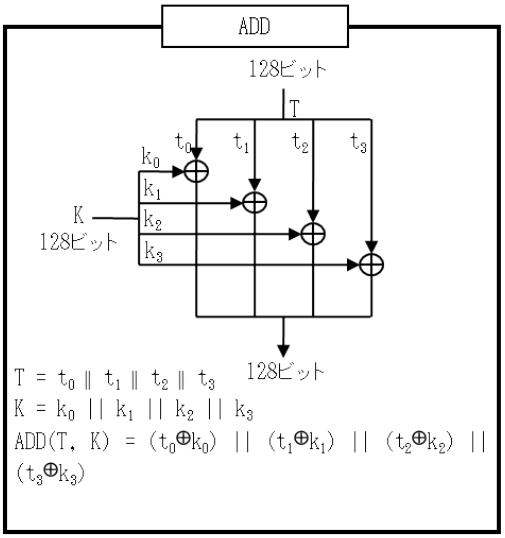
$T = t_0 \| t_1 \| t_2 \| t_3$
$a = Rot_8(t_3)$
$w_0 = SW(a) \oplus t_0 \oplus Rcon$
$w_1 = w_0 \oplus t_1$
$w_2 = w_1 \oplus t_2$
$w_3 = w_2 \oplus t_3$
$KR(T, Rcon) = w_0 \| w_1 \| w_2 \| w_3$



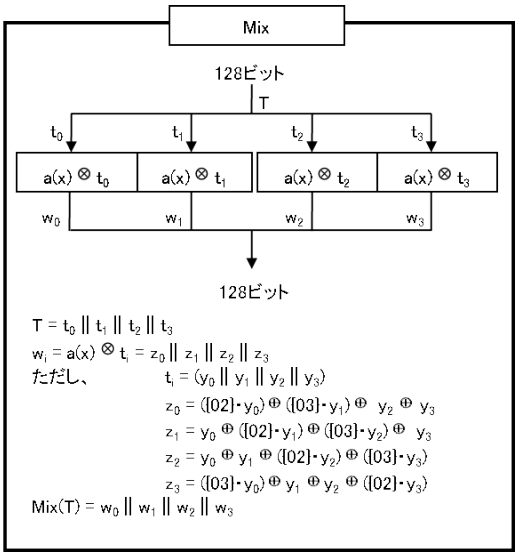
$T = t_0 \| t_1 \| t_2 \| t_3$
$Sub(T) = SW(t_0) \| SW(t_1) \| SW(t_2) \| SW(t_3)$



$S = s_0 \| s_1 \| s_2 \| s_3 \| s_4 \| \cdots \| s_{15}$
$P(S) = a_0 \| a_1 \| a_2 \| a_3$
ただし　$a_0 = (s_0 \| s_4 \| s_8 \| s_{12})$
$a_1 = (s_1 \| s_5 \| s_9 \| s_{13})$
$a_2 = (s_2 \| s_6 \| s_{10} \| s_{14})$
$a_3 = (s_3 \| s_7 \| s_{11} \| s_{15})$
$B = a_0 \| Rot_8(a_1) \| Rot_{16}(a_2) \| Rot_{24}(a_3)$
$Shift(S) = P^{-1}(B)$
$= s_0 \| s_5 \| s_{10} \| s_{15} \| s_4 \| s_9 \| s_{14} \| s_3 \|$
$s_8 \| s_{13} \| s_2 \| s_7 \| s_{12} \| s_1 \| s_6 \| s_{11}$



$T = t_0 \| t_1 \| t_2 \| t_3$
$K = k_0 \| k_1 \| k_2 \| k_3$
$ADD(T, K) = (t_0 \oplus k_0) \| (t_1 \oplus k_1) \| (t_2 \oplus k_2) \| (t_3 \oplus k_3)$



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

注1　Tは、基本関数への入力とする。
2　⊕は、ビットごと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。

別記第３　アルゴリズム定数

R_{con}［１］＝01000000

R_{con}［２］＝02000000

R_{con}［３］＝04000000

R_{con}［４］＝08000000

R_{con}［５］＝10000000

R_{con}［６］＝20000000

R_{con}［７］＝40000000

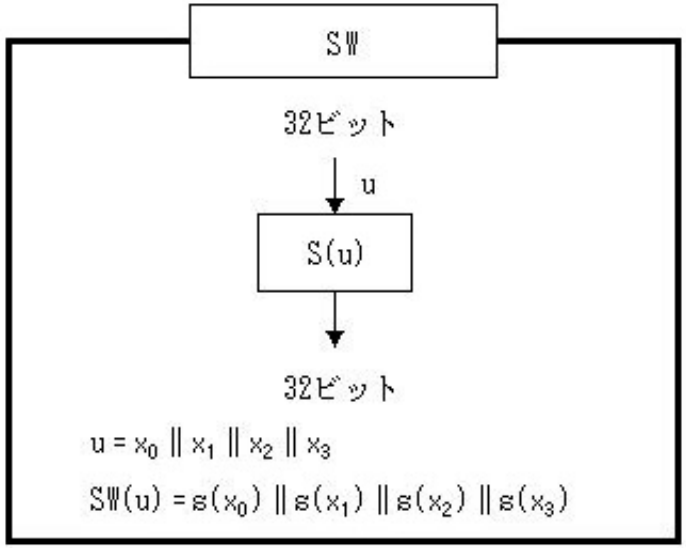
R_{con}［８］＝80000000

R_{con}［９］＝1b000000

R_{con}［10］＝36000000

注　数値は16進数表記とする。

別記第４　補助関数

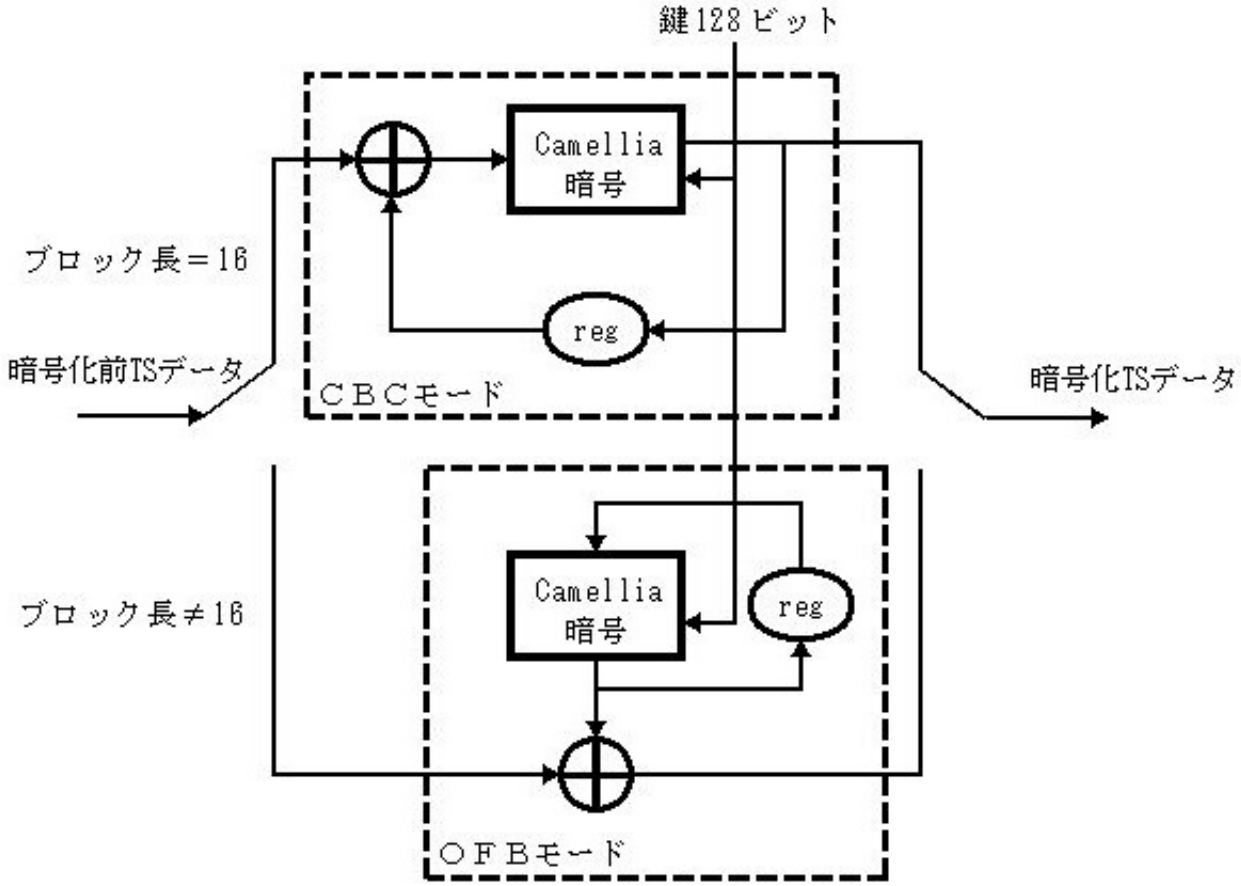


注１　ｕは、補助関数への入力とする。

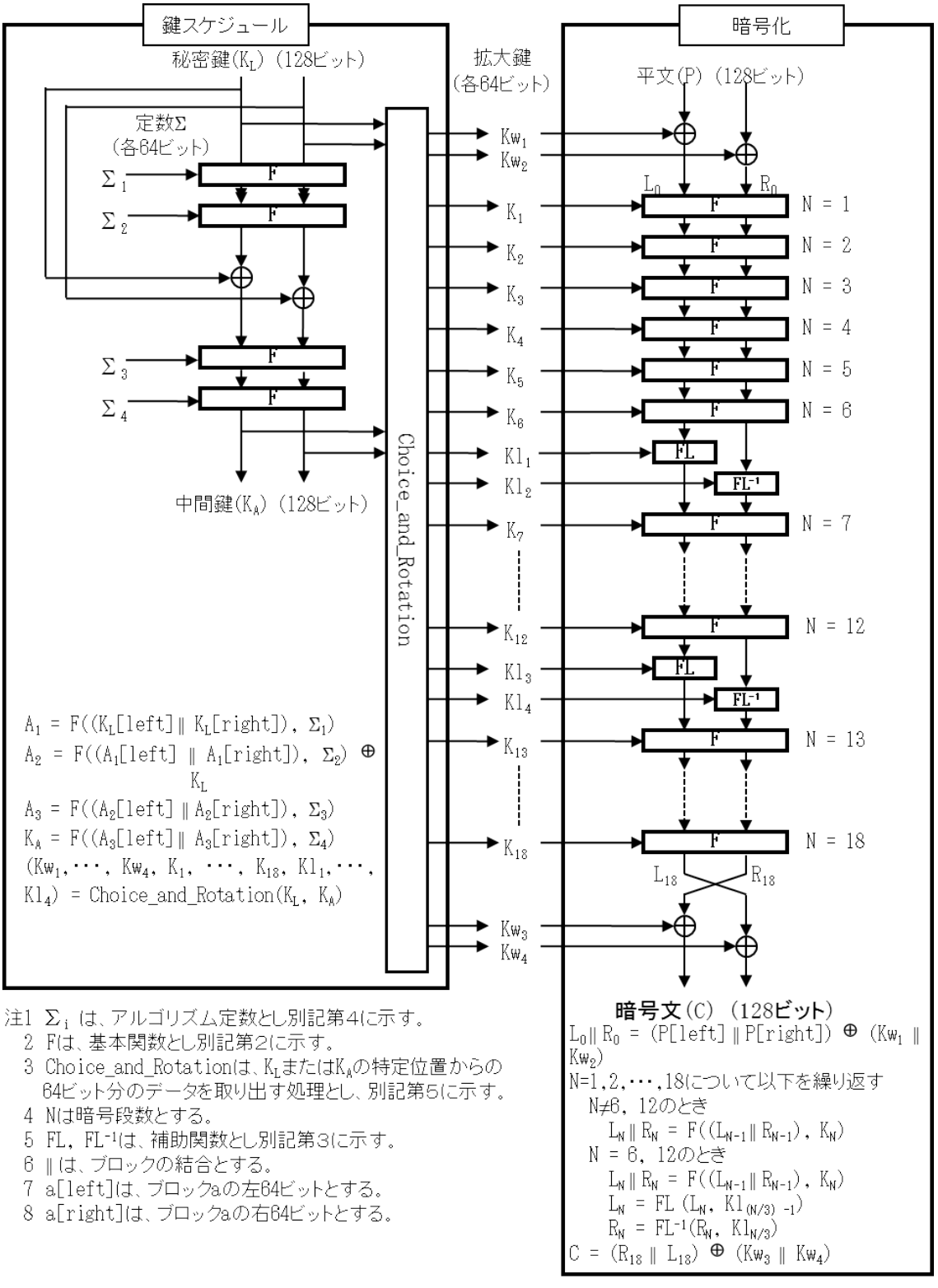
２　||は、ブロックの結合とする。

３　ｓは、８ビットの置換表とし、ＩＳＯ／ＩＥＣ18033-3に従うものとする。

別表第三号

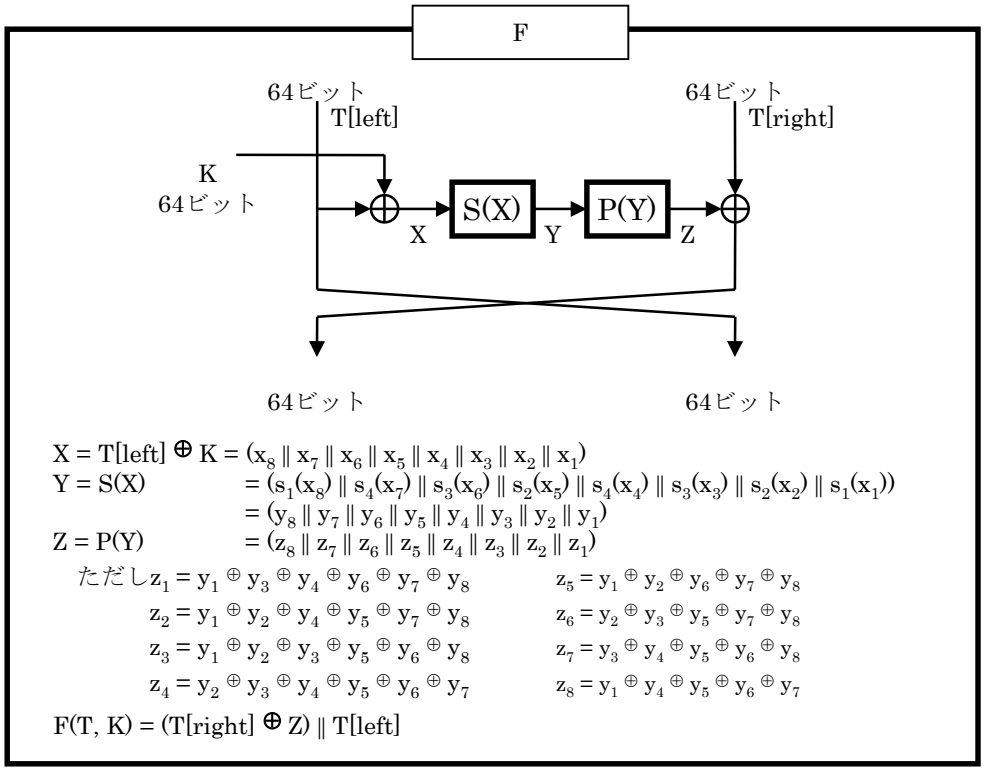


注　Ｃａｍｅｌｌｉａ暗号は、別記第１に示す。



注1 Σ_i は、アルゴリズム定数とし別記第4に示す。
2 Fは、基本関数とし別記第2に示す。
3 Choice_and_Rotationは、K_LまたはK_A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5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。

別記第２　基本関数



$X = T[left] \oplus K = (x_8 \| x_7 \| x_6 \| x_5 \| x_4 \| x_3 \| x_2 \| x_1)$

$Y = S(X) = (s_1(x_8) \| s_4(x_7) \| s_3(x_6) \| s_2(x_5) \| s_4(x_4) \| s_3(x_3) \| s_2(x_2) \| s_1(x_1)) = (y_8 \| y_7 \| y_6 \| y_5 \| y_4 \| y_3 \| y_2 \| y_1)$

$Z = P(Y) = (z_8 \| z_7 \| z_6 \| z_5 \| z_4 \| z_3 \| z_2 \| z_1)$

ただし

$z_1 = y_1 \oplus y_3 \oplus y_4 \oplus y_6 \oplus y_7 \oplus y_8$　　$z_5 = y_1 \oplus y_2 \oplus y_6 \oplus y_7 \oplus y_8$

$z_2 = y_1 \oplus y_2 \oplus y_4 \oplus y_5 \oplus y_7 \oplus y_8$　　$z_6 = y_2 \oplus y_3 \oplus y_5 \oplus y_7 \oplus y_8$

$z_3 = y_1 \oplus y_2 \oplus y_3 \oplus y_5 \oplus y_6 \oplus y_8$　　$z_7 = y_3 \oplus y_4 \oplus y_5 \oplus y_6 \oplus y_8$

$z_4 = y_2 \oplus y_3 \oplus y_4 \oplus y_5 \oplus y_6 \oplus y_7$　　$z_8 = y_1 \oplus y_4 \oplus y_5 \oplus y_6 \oplus y_7$

$F(T, K) = (T[right] \oplus Z) \| T[left]$

注１　Ｔは、基本関数への入力とする。

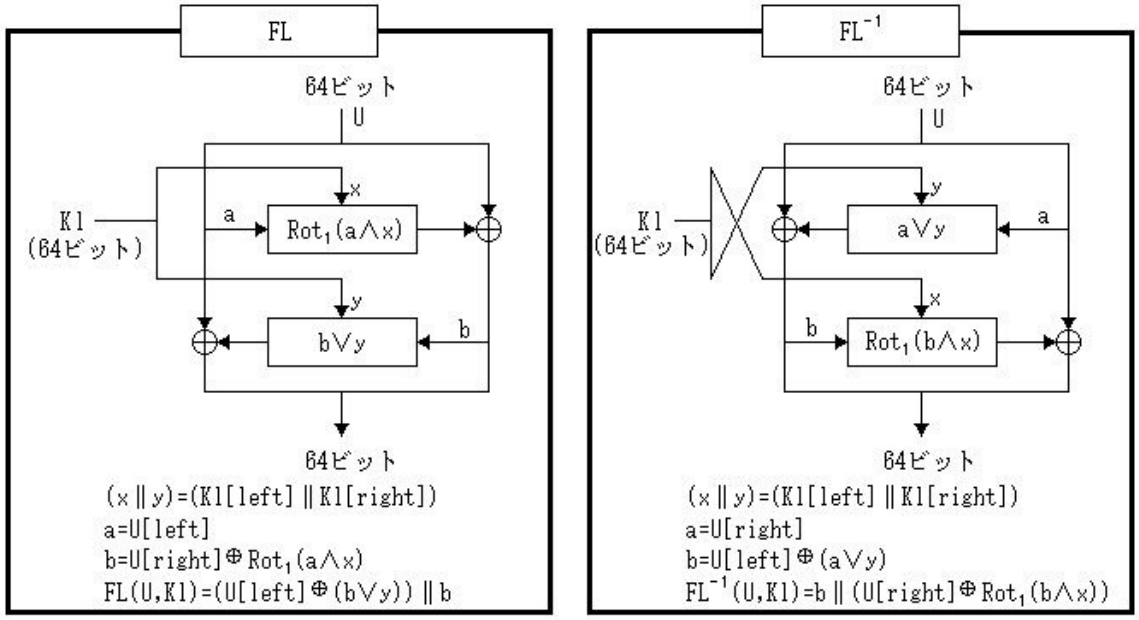
２　Ｔ［ｌｅｆｔ］は、ブロックＴの左64ビットとする。

３　Ｔ［ｒｉｇｈｔ］は、ブロックＴの右64ビットとする。

４　||は、ブロックの結合とする。

５　s_iは、８ビットの置換表とし、ＩＳＯ／ＩＥＣ18033-3:2005（Ｅ）5.2.3.4節に従うこととする。

別記第３　補助関数



注１　Ｕは、基本関数への入力とする。

２　||は、ブロックの結合とする。

３　Ｒｏｔ$_1$は、左巡回１ビットシフトとする。

４　∧は、ビットごとの論理積とする。

５　∨は、ビットごとの論理和とする。

６　Ｕ［ｌｅｆｔ］は、ブロックＵの左32ビットとする。

７　Ｕ［ｒｉｇｈｔ］は、ブロックＵの右32ビットとする。

別記第４　アルゴリズム定数

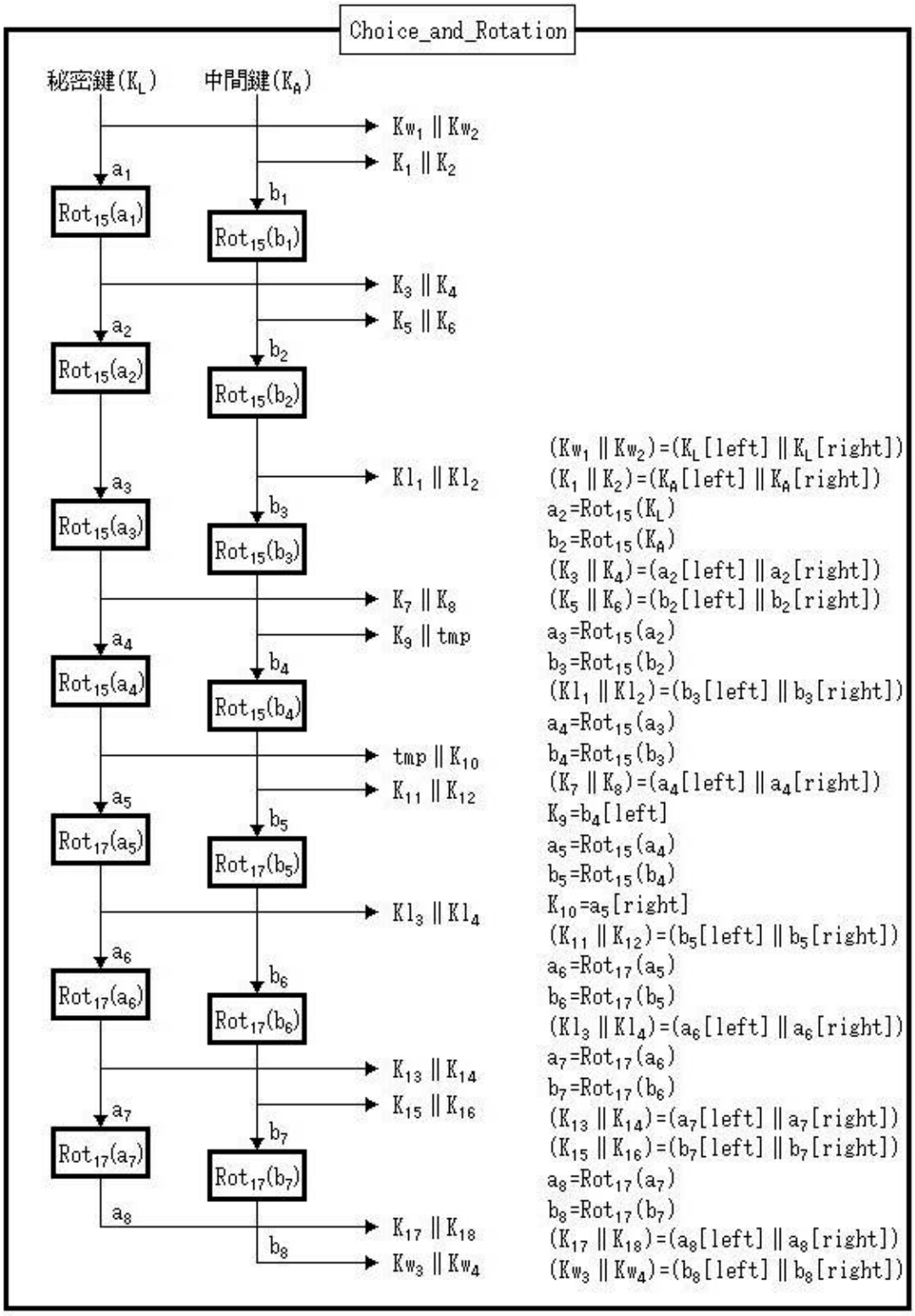
Σ_1＝a09e667f3bcc908b

Σ_2＝b67ae8584caa73b2

Σ_3＝c6ef372fe94f82be

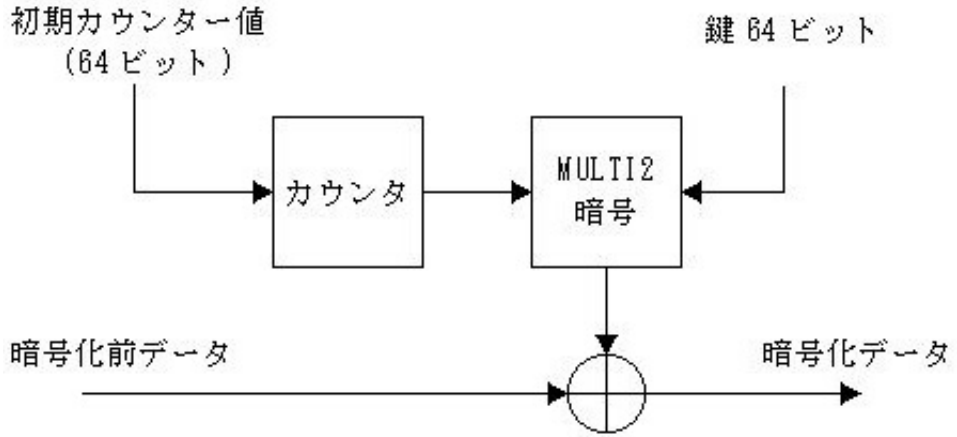
Σ_4＝54ff53a5f1d36f1c

注　数値は16進数表記とする。



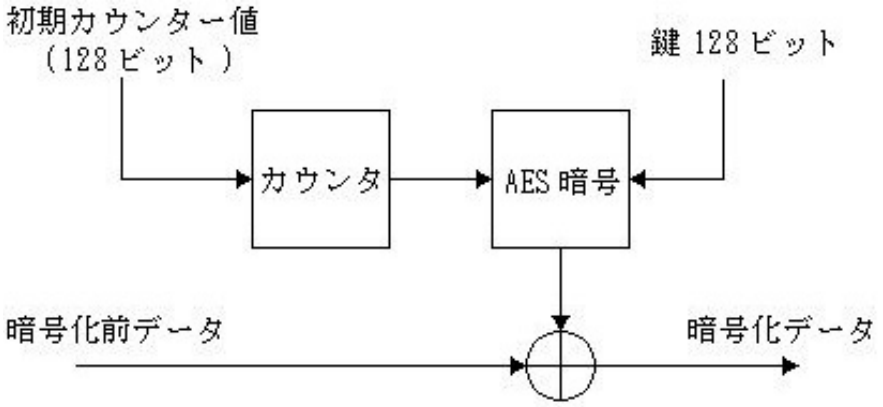
注1　Rot_nは、左巡回nビットシフトとする。
　2　$\|$は、ブロックの結合とする。
　3　U［left］は、ブロックUの左64ビットとする。
　4　U［right］は、ブロックUの右64ビットとする。

別表第四号



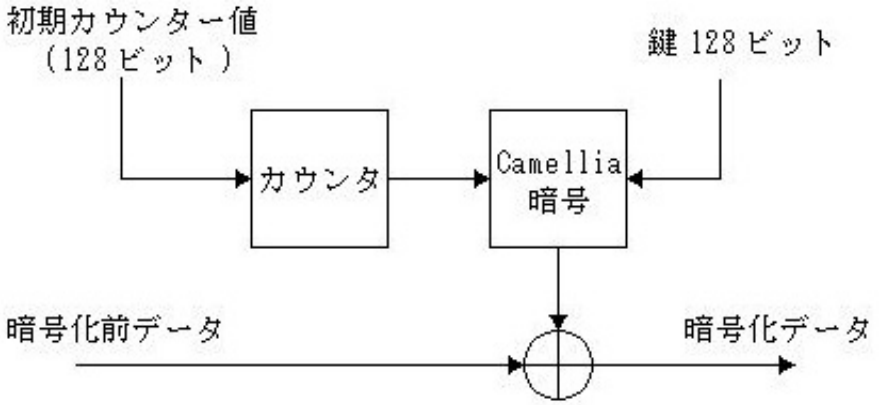
注　ＭＵＬＴＩ２暗号は、別表第一号別記第１に示す。

別表第五号



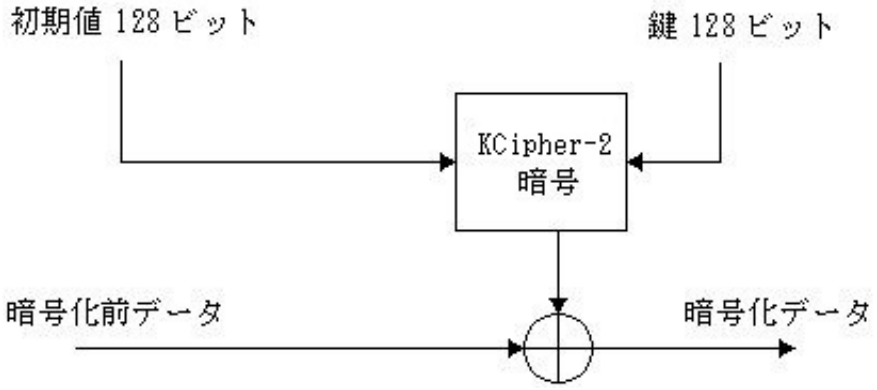
注　ＡＥＳ暗号は、別表第二号別記第１に示す。

別表第六号



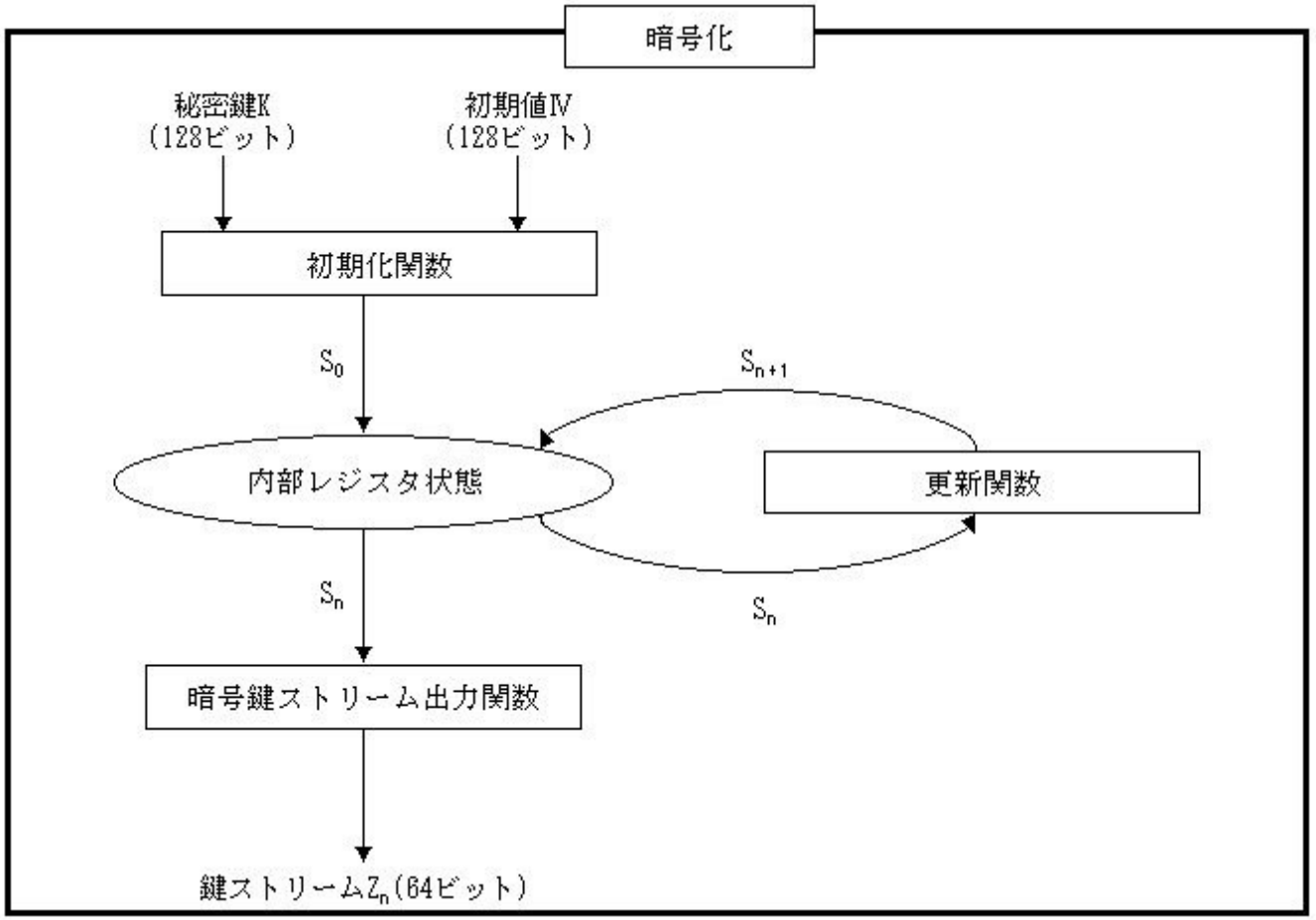
注　Ｃａｍｅｌｌｉａ暗号は、別表第三号別記第１に示す。

別表第七号



注　ＫＣｉｐｈｅｒ－２暗号は、別記第１に示す。

別記第１　ＫＣｉｐｈｅｒ－２暗号

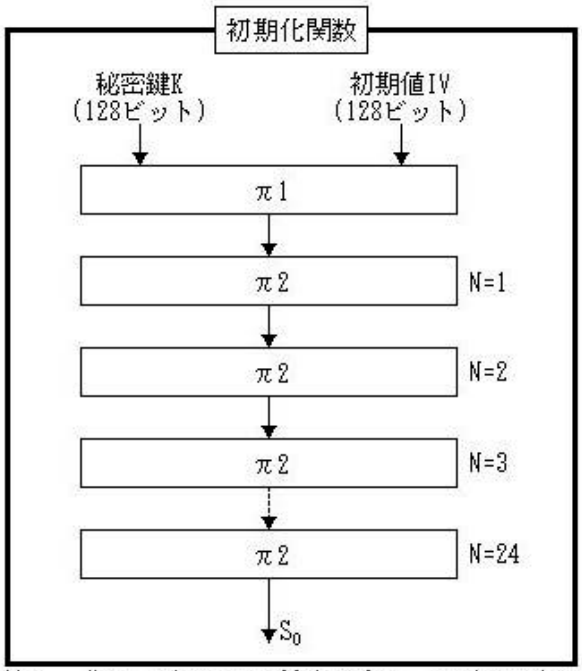


注１　初期化関数は、別記第２に示す。

２　S_nは内部レジスタ状態を示すものとする。

３　更新関数は、別記第３に示す。

４　暗号鍵ストリーム出力関数は、別記第４に示す。



注1　‖は、ブロックの結合とする。以下この表において同じ。

2　x<<nは、xのnビット左巡回シフト、x>>nはxのnビット右巡回シフトを示すものとする。以下この表において同じ。

3　A_0からA_4まで、B_0からB_{10}まで、R1、L1、R2及びL2は32ビットの値を示す変数とする。

4　「0x」に続く数字を16進数とする。以下この表において同じ。

5　$+_{32}$及び⊗は、それぞれGF(2^{32})上の算術加算と乗算を示すものとする。以下この表において同じ。

6　Sub_{K2}は、別表第2号に示すSW関数・Mix関数を順に適用する関数とする。以下この表において同じ。

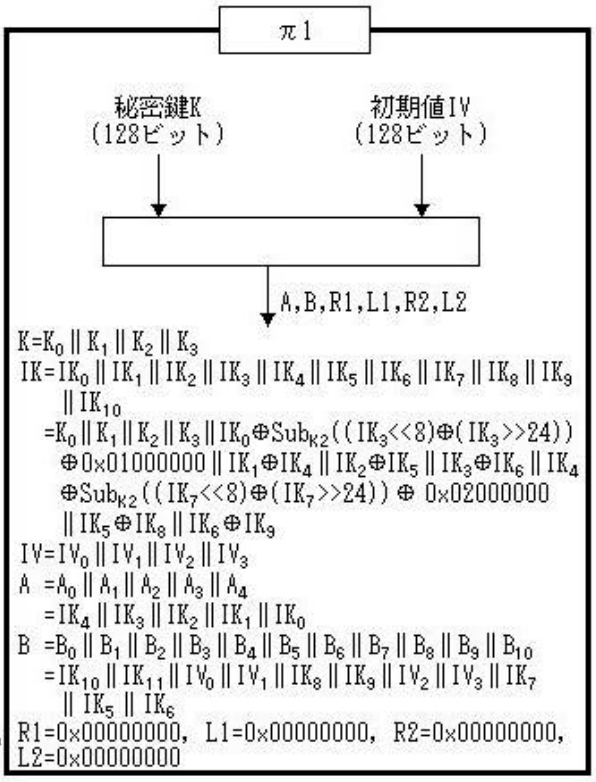
7　α_0は、GF(2^{32})上の元であり、$\chi^4+\beta^{24}\chi^3+\beta^3\chi^2+\beta^{12}\chi+\beta^{71}\in GF(2^8)[\chi]$の根とする。ただし、$\beta$は原始多項式$\chi^8+\chi^7+\chi^6+\chi+1\in GF(2)[\chi]$の根とする。以下この表において同じ。

8　α_1はGF(2^{32})上の元であり$\chi^4+\gamma^{230}\chi^3+\gamma^{156}\chi^2+\gamma^{93}\chi+\gamma^{29}\in GF(2^8)[\chi]$の根とする。ただし、$\gamma$は原始多項式$\chi^8+\chi^5+\chi^3+\chi^2+1\in GF(2)[\chi]$の根とする。以下この表において同じ。

9　X[Y]は、XのY番目のビットを示すものとする。以下この表において同じ。

10　α_2はGF(2^{32})上の元であり$\chi^4+\delta^{34}\chi^3+\delta^{16}\chi^2+\delta^{199}\chi+\delta^{248}\in GF(2^8)[\chi]$の根とする。ただし、$\delta$は原始多項式$\chi^8+\chi^6+\chi^3+\chi^2+1\in GF(2)[\chi]$の根とする。以下この表において同じ。

11　α_3はGF(2^{32})上の元であり$\chi^4+\xi^{157}\chi^3+\xi^{253}\chi^2+\xi^{56}\chi+\xi^{16}\in GF(2^8)[\chi]$の根とする。ただし、$\xi$は原始多項式$\chi^8+\chi^6+\chi^5+\chi^2+1\in GF(2)[\chi]$の根とする。以下この表において同じ。



$K=K_0\|K_1\|K_2\|K_3$

$IK=IK_0\|IK_1\|IK_2\|IK_3\|IK_4\|IK_5\|IK_6\|IK_7\|IK_8\|IK_9\|IK_{10}$

$=K_0\|K_1\|K_2\|K_3\|IK_0\oplus Sub_{K2}((IK_3<<8)\oplus(IK_3>>24))\oplus 0x01000000\|IK_1\oplus IK_4\|IK_2\oplus IK_5\|IK_3\oplus IK_6\|IK_4\oplus Sub_{K2}((IK_7<<8)\oplus(IK_7>>24))\oplus 0x02000000\|IK_5\oplus IK_8\|IK_6\oplus IK_9$

$IV=IV_0\|IV_1\|IV_2\|IV_3$

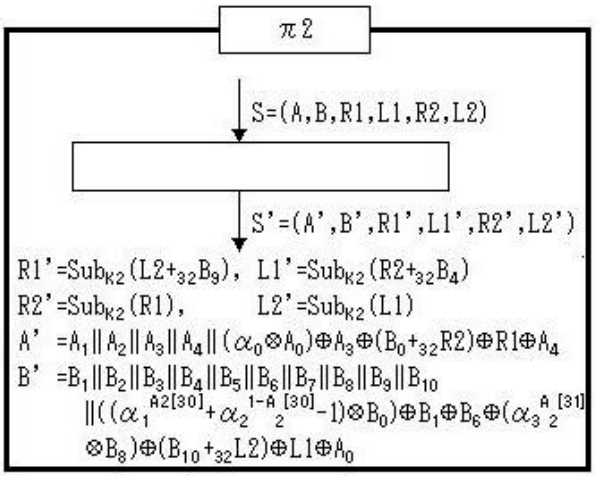
$A=A_0\|A_1\|A_2\|A_3\|A_4$

$=IK_4\|IK_3\|IK_2\|IK_1\|IK_0$

$B=B_0\|B_1\|B_2\|B_3\|B_4\|B_5\|B_6\|B_7\|B_8\|B_9\|B_{10}$

$=IK_{10}\|IK_{11}\|IV_0\|IV_1\|IK_8\|IK_9\|IV_2\|IV_3\|IK_7\|IK_5\|IK_6$

R1=0x00000000, L1=0x00000000, R2=0x00000000, L2=0x00000000



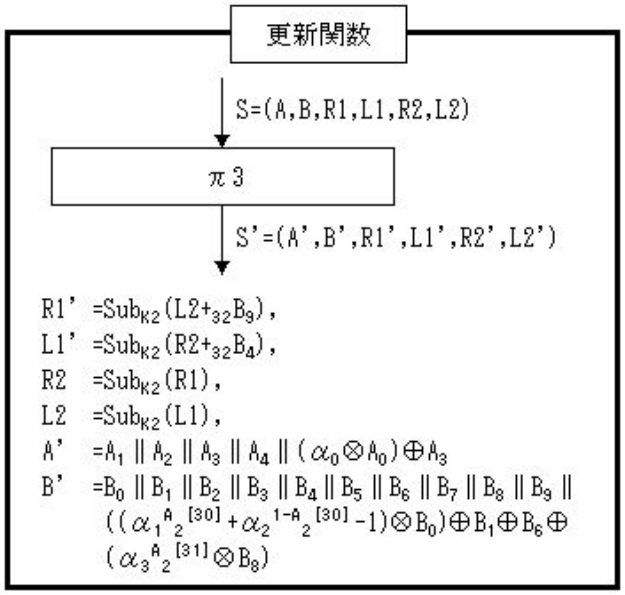
$R1'=Sub_{K2}(L2+_{32}B_9)$, $L1'=Sub_{K2}(R2+_{32}B_4)$

$R2'=Sub_{K2}(R1)$, $L2'=Sub_{K2}(L1)$

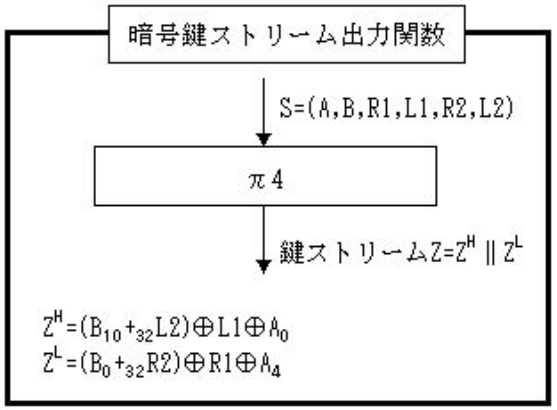
$A'=A_1\|A_2\|A_3\|A_4\|(\alpha_0\otimes A_0)\oplus A_3\oplus(B_0+_{32}R2)\oplus R1\oplus A_4$

$B'=B_1\|B_2\|B_3\|B_4\|B_5\|B_6\|B_7\|B_8\|B_9\|B_{10}\|((\alpha_1^{A2[30]}+\alpha_2^{1-A2[30]}-1)\otimes B_0)\oplus B_1\oplus B_6\oplus(\alpha_3^{A2[31]}\otimes B_8)\oplus(B_{10}+_{32}L2)\oplus L1\oplus A_0$

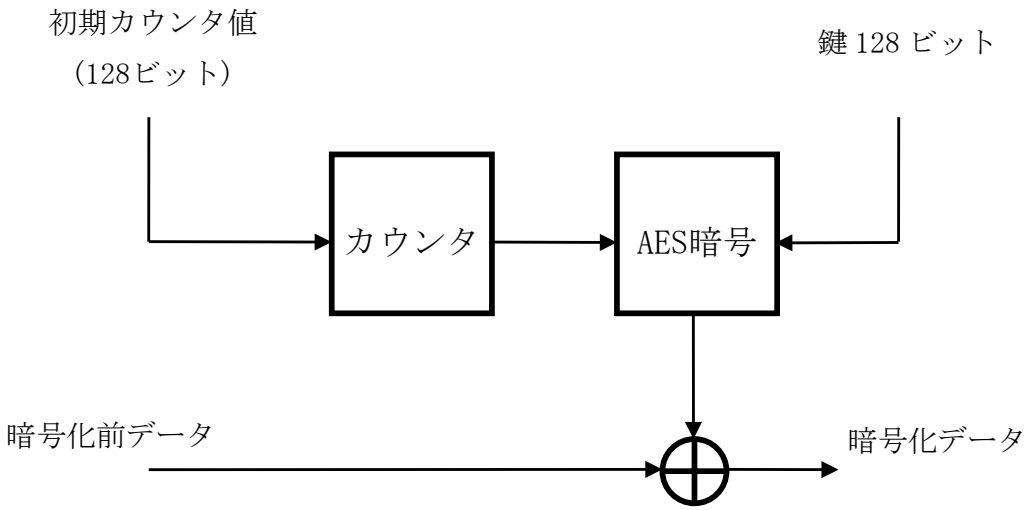
別記第３　更新関数



別記第４　暗号鍵ストリーム出力関数

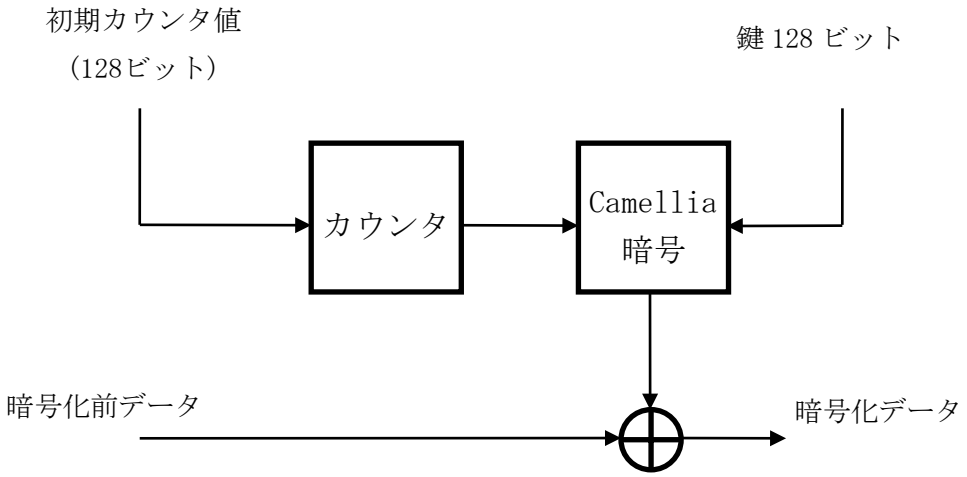


別表第八号



注　ＡＥＳ暗号は、別表第二号別記第１に示す。

別表第九号



注　Ｃａｍｅｌｌｉａ暗号は、別表第三号別記第１に示す。