別添8

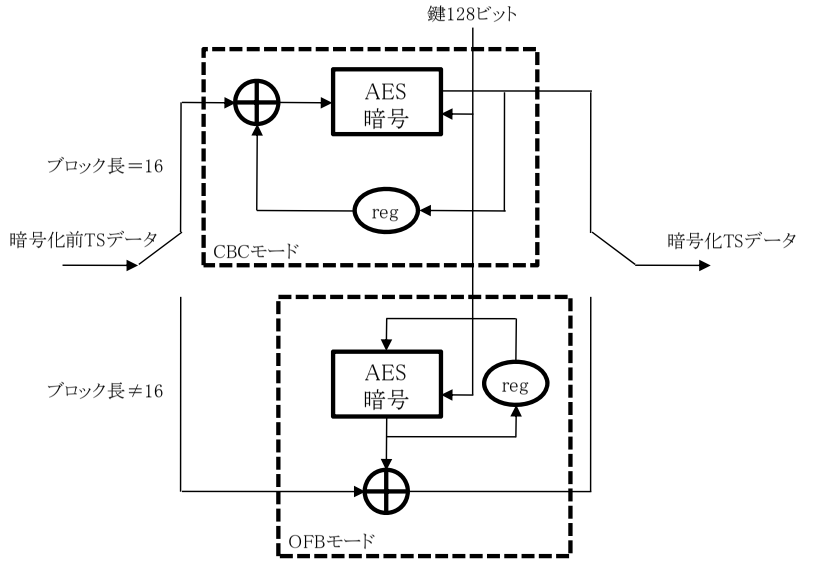
スクランブルの方式を定める件の一部を改正する告示案新旧対照表

○　スクランブルの方式を定める件（平成十五年総務省告示第四十号）

（傍線部分は改正部分）

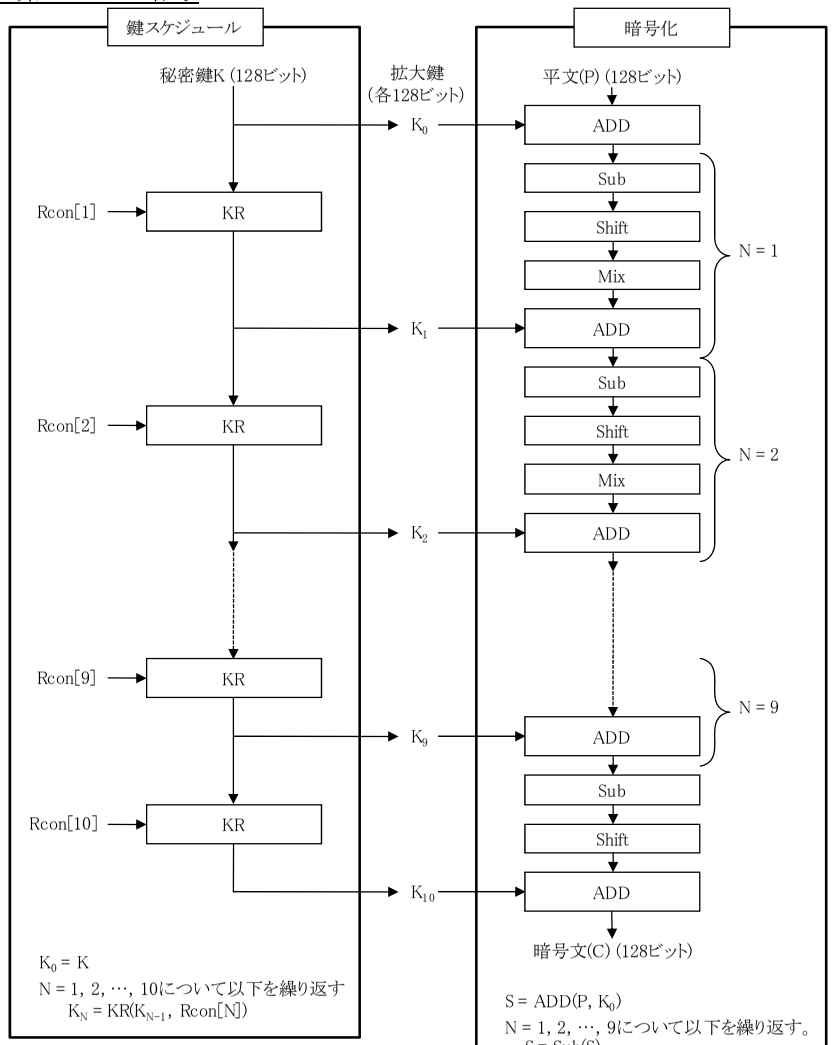
改正案	現行
1　標準テレビジョン放送等のうちデジタル放送に関する送信の標準方式（以下「標準方式」という。）第八条第一号の規定に基づくスクランブルの方式は次の各号に掲げるとおりとする。	1　標準テレビジョン放送等のうちデジタル放送に関する送信の標準方式（以下「標準方式」という。）第八条第一号の規定に基づくスクランブルの方式は以下のとおりとする。
一　スクランブルの範囲は、ＴＳパケット（伝送制御信号及び関連情報を送るためのものを除く。）のペイロード部とする。	一　スクランブルの範囲は、ＴＳパケット（伝送制御信号及び関連情報を送るためのものを除く。）のペイロード部とする。
二　スクランブルの手順は、別表第一号のとおりとする。	二　スクランブルの手順は、別表第一号のとおりとする。
三　標準方式第三章の二第一節に規定す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のいずれかとする。	
2　（略）	2　（略）
3　標準方式第二十二条の二十四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のいずれかとする。	
別表第一号　（略図） 注１　ＭＵＬＴＩ２暗号は、別記第１に示す。 ２　reg は、レジスターを示す。以下同じ。 ３　⊕は、排他的論理和を示す。以下同じ。	別表第一号　（略図） 注１　ＭＵＬＴＩ２暗号は、別記第１に示す。 ２　reg は、レジスターを示す。 ３　⊕は、排他的論理和を示す。
別記第１　（略）	別記第１　（略）
別記第２　（略図） 注１～３　（略）	別記第２　（略図） 注１～３　（略） ４　⊕は、ビット毎の排他的論理和とする。
４～８　（略）	５～９　（略）

別表第二号



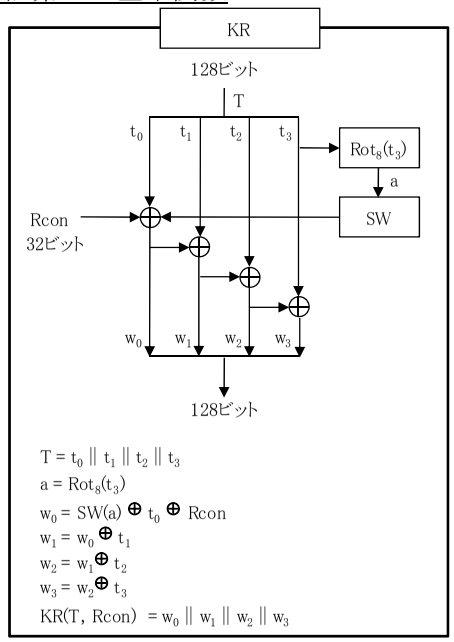
注１　AES暗号は、別記第１に示す。

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。

別記第２　基本関数



$T = t_0 \| t_1 \| t_2 \| t_3$

$a = Rot_8(t_3)$

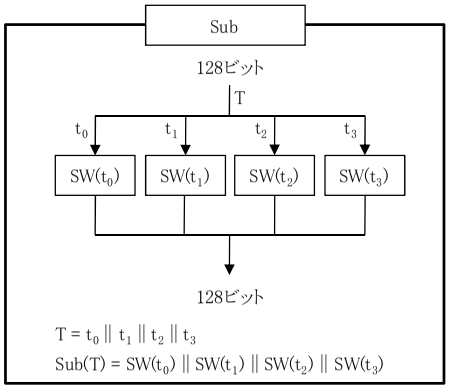
$w_0 = SW(a) \oplus t_0 \oplus Rcon$

$w_1 = w_0 \oplus t_1$

$w_2 = w_1 \oplus t_2$

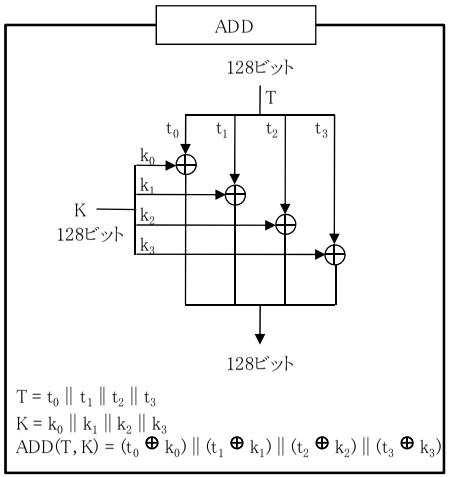
$w_3 = w_2 \oplus t_3$

$KR(T, Rcon) = w_0 \| w_1 \| w_2 \| w_3$



$T = t_0 \| t_1 \| t_2 \| t_3$

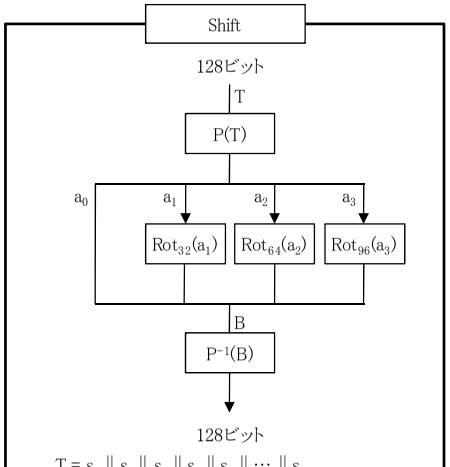
$Sub(T) = SW(t_0) \| SW(t_1) \| SW(t_2) \| SW(t_3)$



$T = t_0 \| t_1 \| t_2 \| t_3$

$K = k_0 \| k_1 \| k_2 \| k_3$

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



$T = s_0 \| s_1 \| s_2 \| s_3 \| s_4 \| \cdots \| s_{15}$

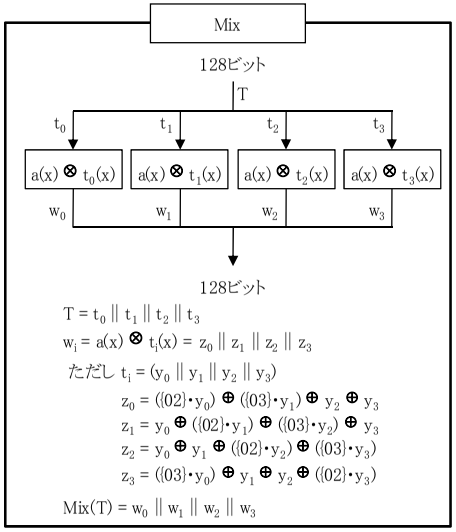
$P(T) = a_0 \| a_1 \| a_2 \| a_3$

ただし $a_0 = (s_0 \| s_4 \| s_8 \| s_{12})$
$a_1 = (s_1 \| s_5 \| s_9 \| s_{13})$
$a_2 = (s_2 \| s_6 \| s_{10} \| s_{14})$
$a_3 = (s_3 \| s_7 \| s_{11} \| s_{15})$

$B = a_0 \| Rot_{32}(a_1) \| Rot_{64}(a_2) \| Rot_{96}(a_3)$

$Shift(T) = P^{-1}(B)$
$= s_0 \| s_5 \| s_{10} \| s_{15} \| s_4 \| s_9 \| s_{14} \| s_3 \|$
$s_8 \| s_{13} \| s_2 \| s_7 \| s_{12} \| s_1 \| s_6 \| s_{11}$

注１　T 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_n は、左巡回nビットシフトとする。
　４　SWは、補助関数とし別記第４に示す。
　５　{}内は、16進数表記とする。
　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。

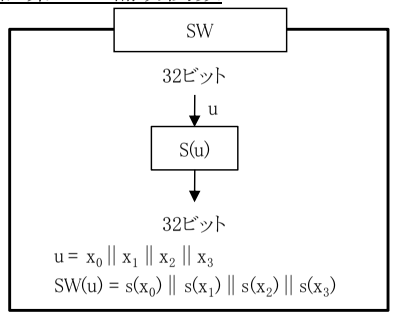


別記第３　アルゴリズム定数

Rcon[1] = 01000000
Rcon[2] = 02000000
Rcon[3] = 04000000
Rcon[4] = 08000000
Rcon[5] = 10000000
Rcon[6] = 20000000
Rcon[7] = 40000000
Rcon[8] = 80000000
Rcon[9] = 1b000000
Rcon[10] = 36000000

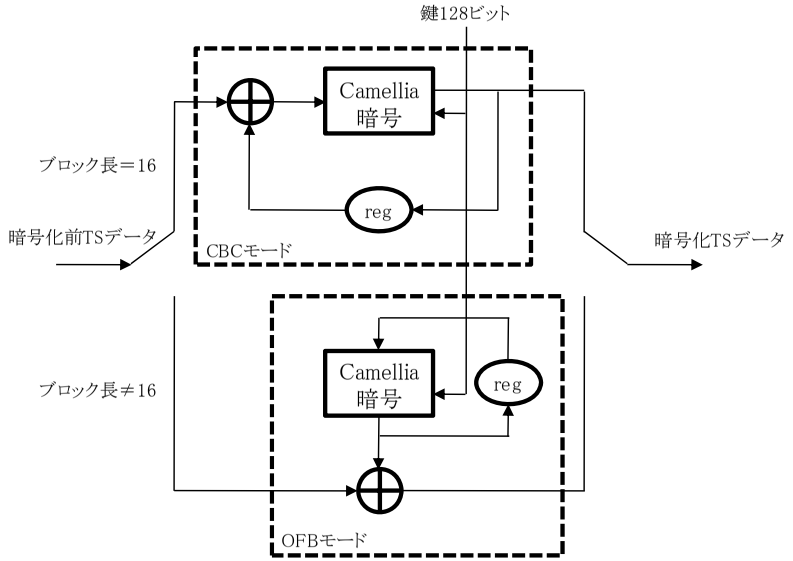
注　数値は16進数表記とする。

別記第４　補助関数



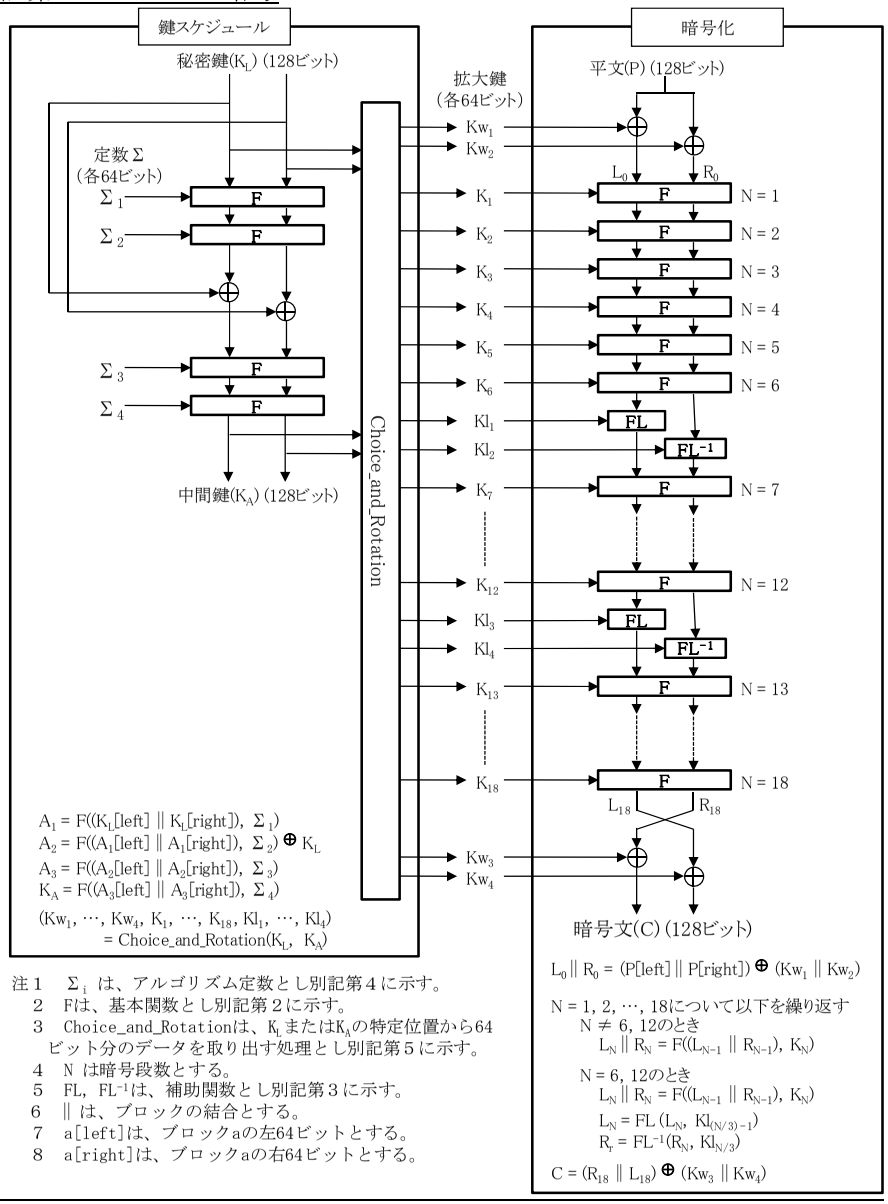
注１　u は、補助関数への入力とする。
　２　||は、ブロックの結合とする。
　３　s は、8ビットの置換表とし、
　　ISO/IEC 18033-3に従うものとする。

別表第三号



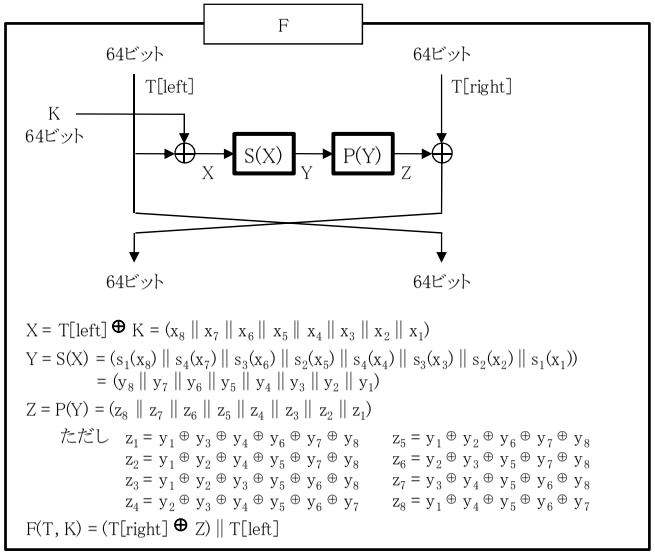
注　Camellia暗号は、別記第１に示す。

別記第１　Camellia暗号



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



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

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

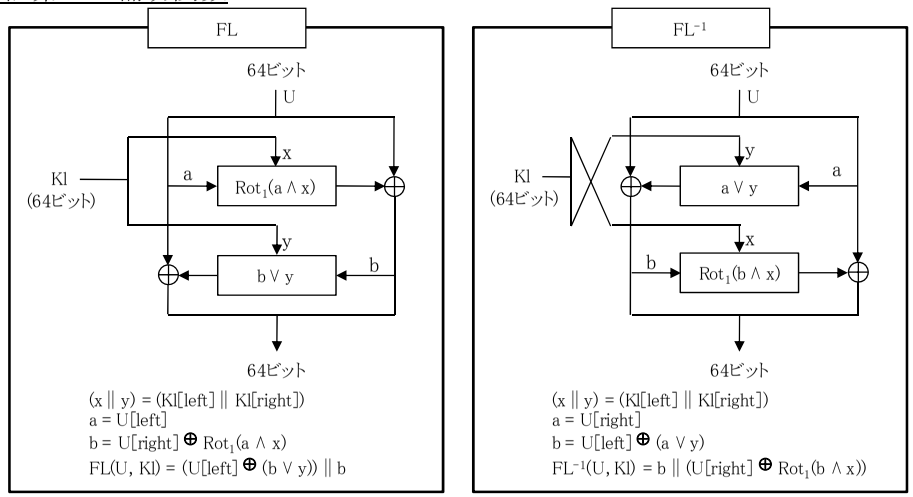
$Z = P(Y) = (z_8 \| z_7 \| z_6 \| z_5 \| z_4 \| z_3 \| z_2 \| z_1)$

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 5.2.3.4節に従うこととする。

別記第３　補助関数

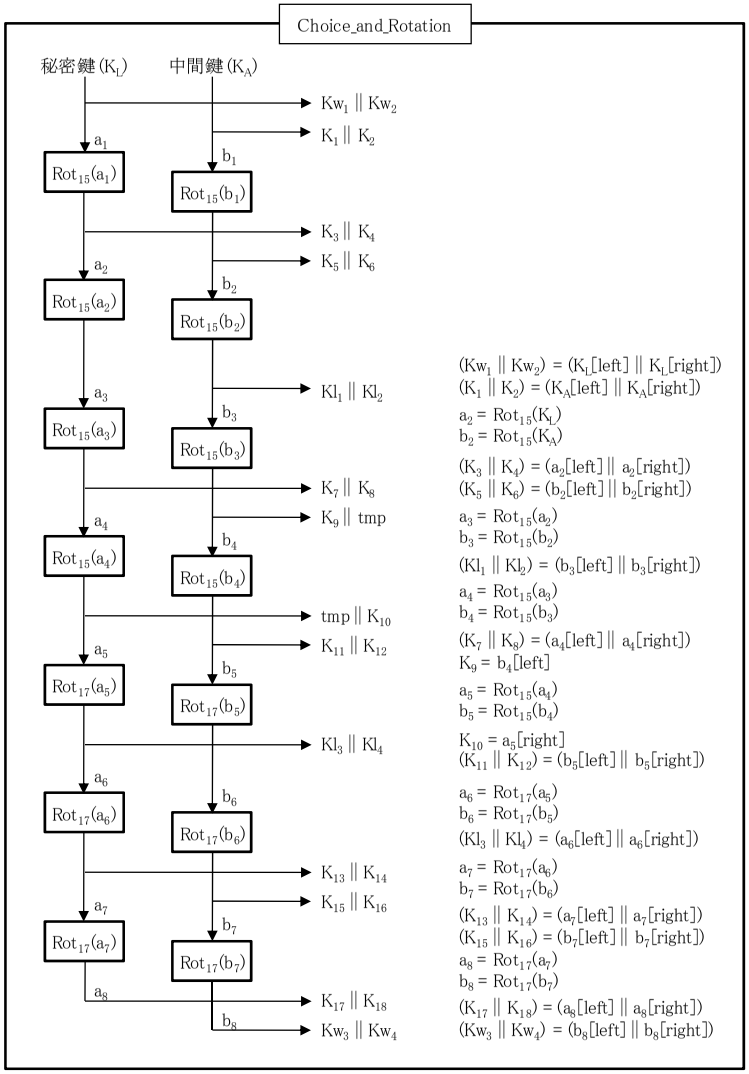


注１　U は、補助関数への入力とする。
　２　‖ は、ブロックの結合とする。
　３　Rot_1 は、左巡回1ビットシフトとする。
　４　∧ は、ビット毎の論理積とする。
　５　∨ は、ビット毎の論理和とする。
　６　U[left]は、ブロックUの左64ビットとする。
　７　U[right]は、ブロックUの右64ビットとする。

別記第４　アルゴリズム定数

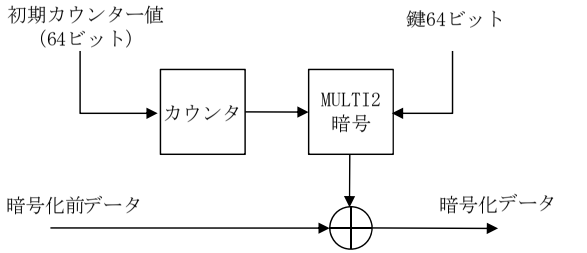
Σ_1 = a09e667f3bcc908b
Σ_2 = b67ae8584caa73b2
Σ_3 = c6ef372fe94f82be
Σ_4 = 54ff53a5f1d36f1c
注　数値は16進数表記とする。

別記第５　Choice_and_Rotation



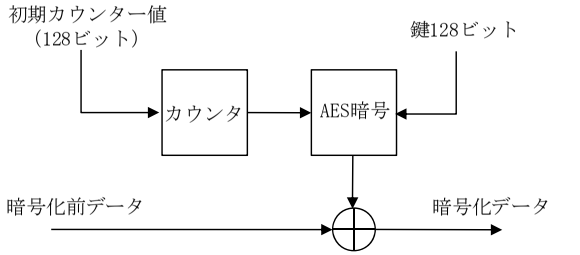
注１　Rot_n は、左巡回nビットシフトとする。
　２　‖は、ブロックの結合とする。
　３　U[left]は、ブロックUの左64ビットとする。
　４　U[right]は、ブロックUの右64ビットとする。

別表第四号



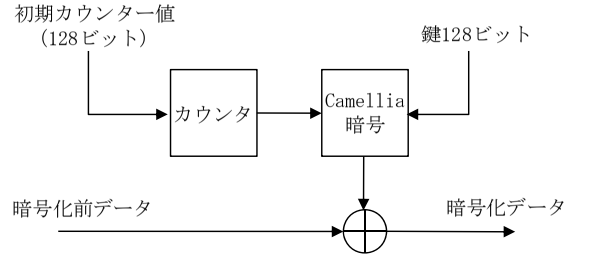
注　MULTI2暗号は、別表第一号別記第１に示す。

別表第五号



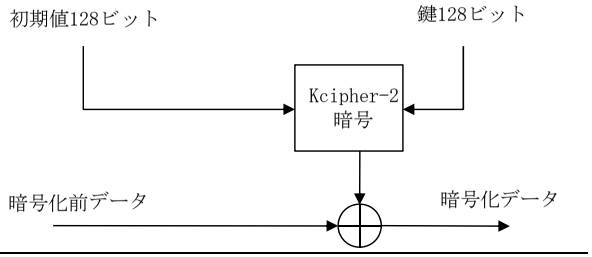
注　AES暗号は、別表第二号別記第１に示す。

別表第六号



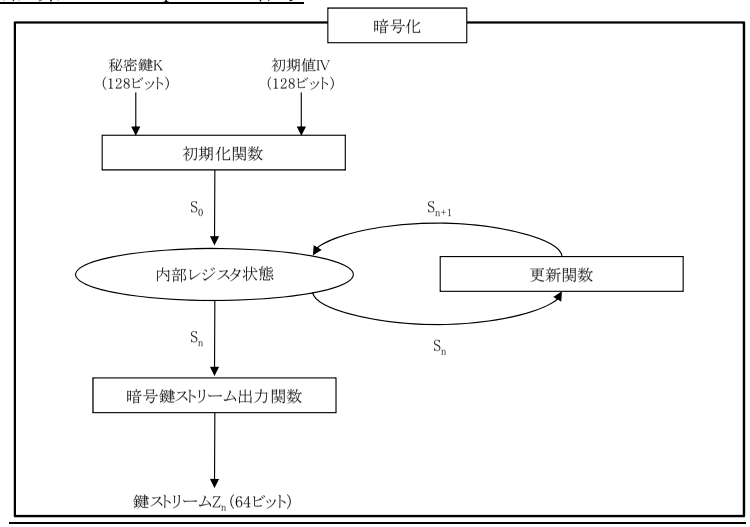
注　Camellia暗号は、別表第三号別記第１に示す。

別表第七号



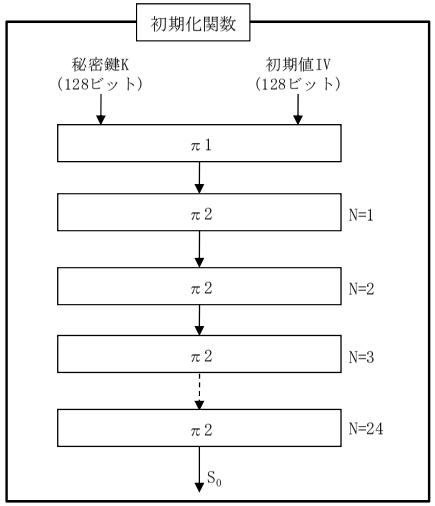
注　KCipher-2暗号は、別記第１に示す。

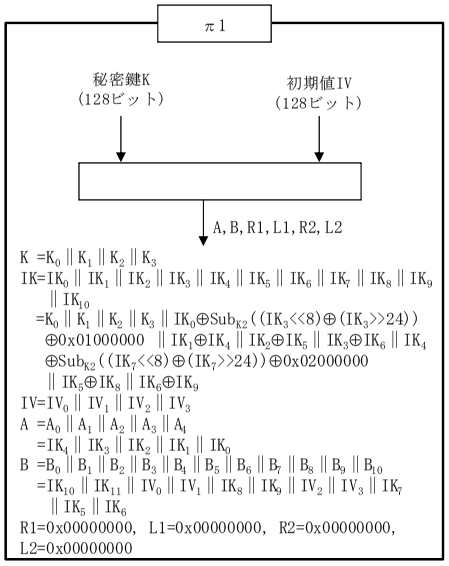
別記第１　KCipher-2暗号

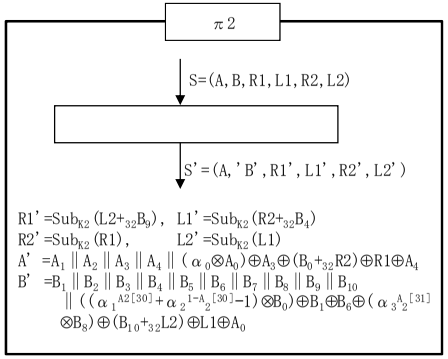


注１　初期化関数は、別記第２に示す。
　２　S_nは、内部レジスタ状態を表すものとする。
　３　更新関数は、別記第３に示す。
　４　暗号鍵ストリーム出力関数は、別記第４に示す。

別記第２　初期化関数







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

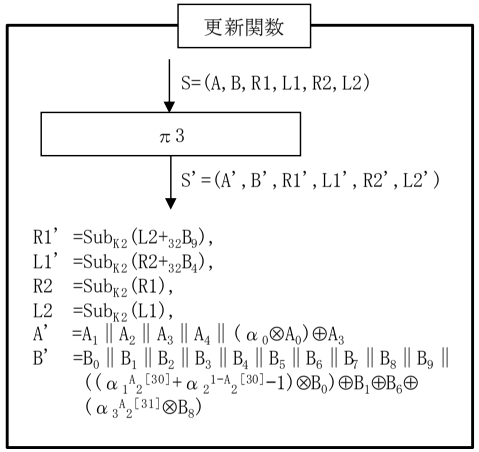
８　α_1はGF(2^{32})上の元であり$x^4+\gamma^{230}x^3+\gamma^{156}x^2+\gamma^{93}x+\gamma^{29}\in GF(2^8)[x]$の根とする。ただし、$\gamma$は原始多項式$x^8+x^6+x^3+x^2+1\in GF(2)[x]$の根とする。以下この表において同じ。

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$x^4+\delta^{34}x^3+\delta^{16}x^2+\delta^{199}x+\delta^{248}\in GF(2^8)[x]$の根とする。ただし、$\delta$は原始多項式$x^8+x^6+x^3+x^2+1\in GF(2)[x]$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$x^4+\zeta^{157}x^3+\zeta^{253}x^2+\zeta^{56}x+\zeta^{16}\in GF(2^8)[x]$の根とする。ただし、$\zeta$は原始多項式$x^8+x^6+x^5+x^2+1\in GF(2)[x]$の根とする。以下この表において同じ。

別記第３　更新関数



別記第４　暗号鍵ストリーム出力関数