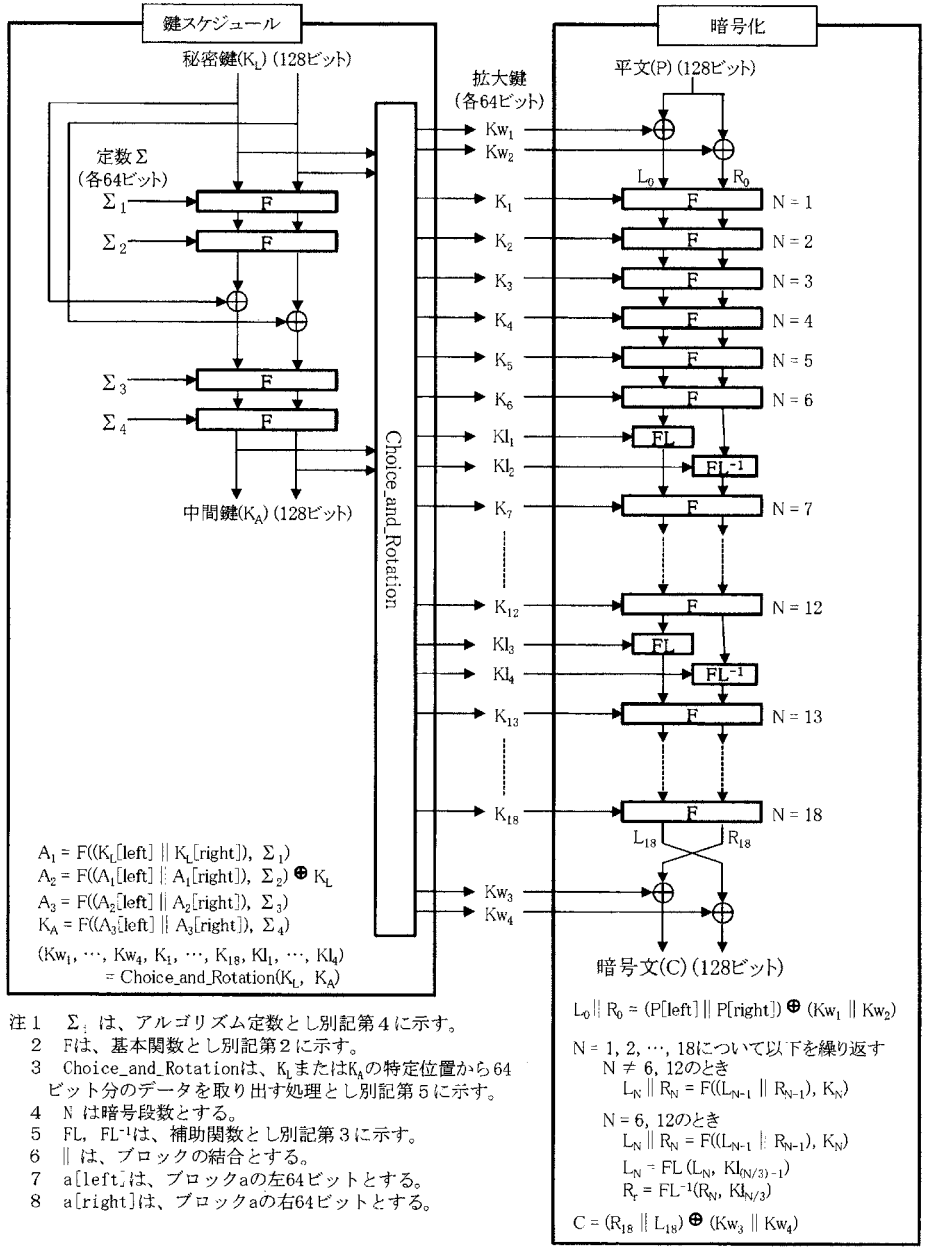
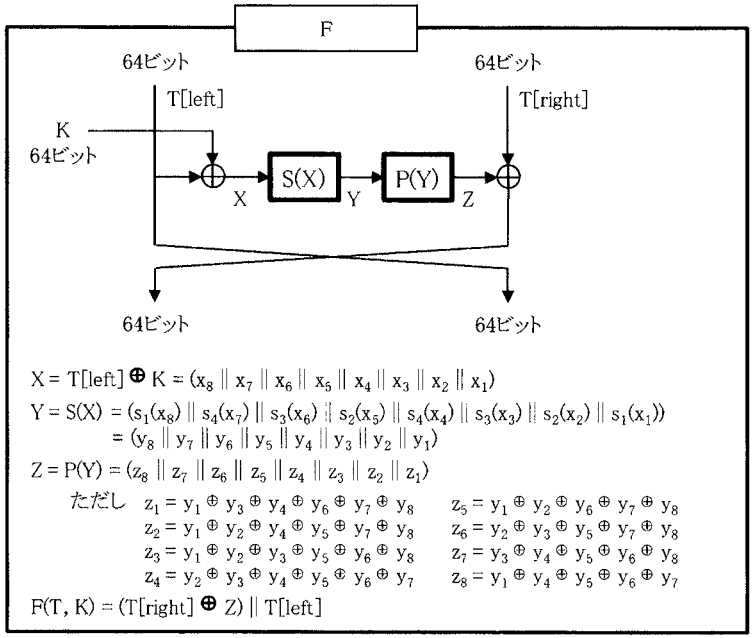
別記第１　Camellia暗号



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。