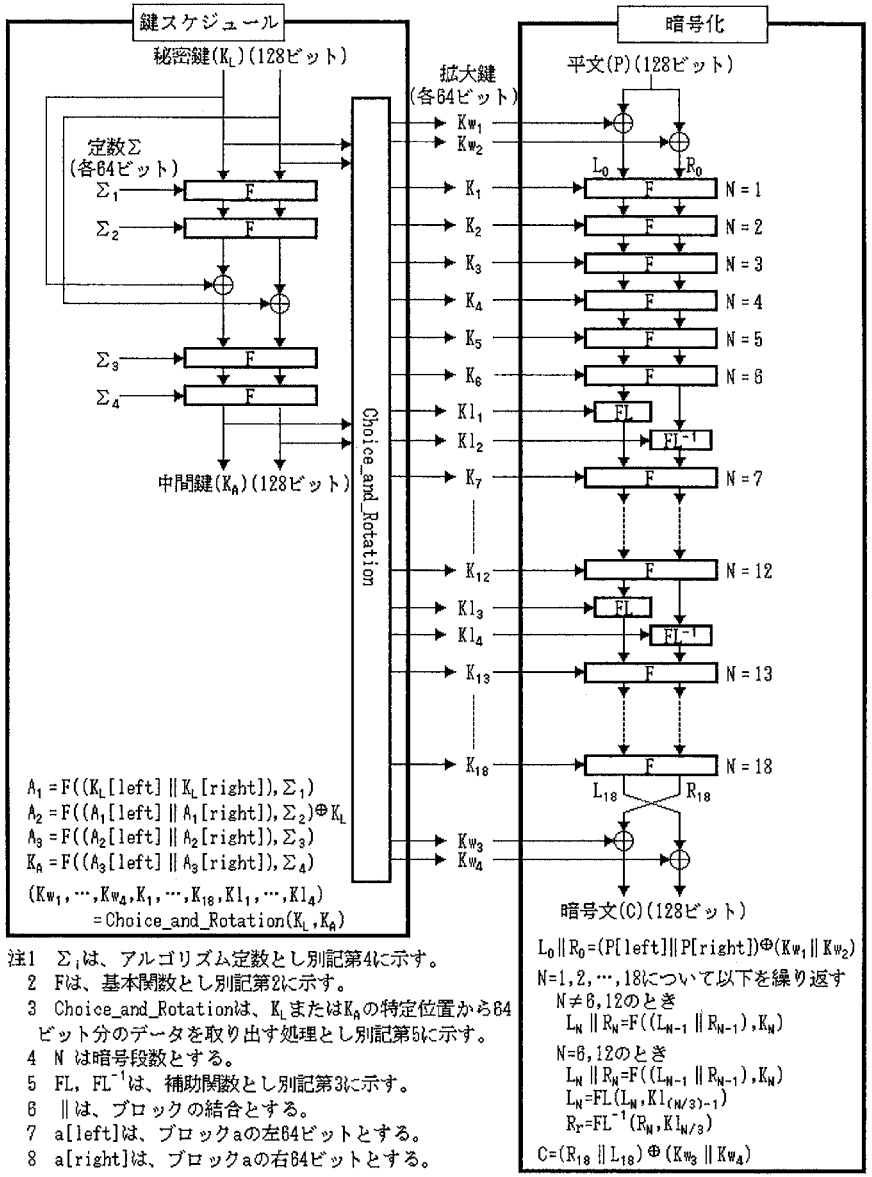
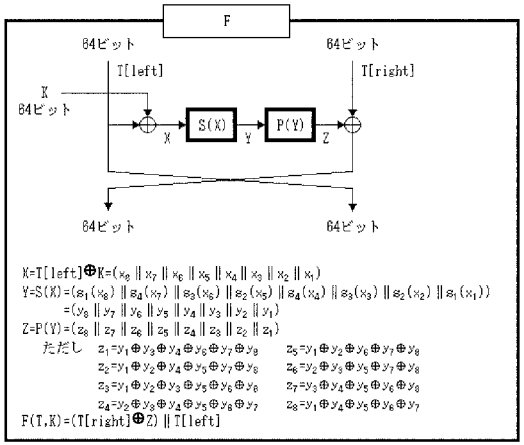
別記第１　Camellia暗号



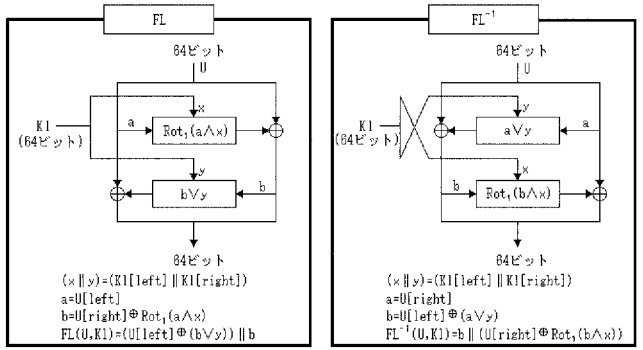
注1　Σ_iは、アルゴリズム定数とし別記第4に示す。
2　Fは、基本関数とし別記第2に示す。
3　Choice_and_Rotationは、K_LまたはK_Aの特定位置から64ビット分のデータを取り出す処理とし別記第5に示す。
4　Nは暗号段数とする。
5　FL，FL^{-1}は、補助関数とし別記第3に示す。
6　‖は、ブロックの結合とする。
7　a[left]は、ブロックaの左64ビットとする。
8　a[right]は、ブロックaの右64ビットとする。

別記第２　基本関数



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、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。