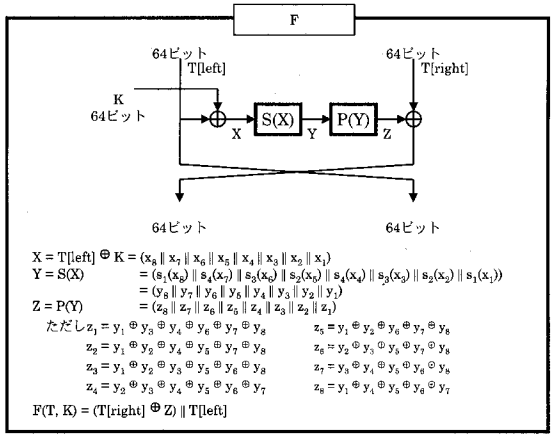
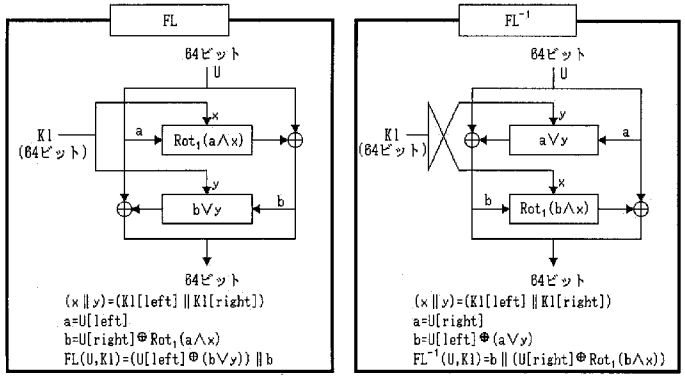
別記第２　基本関数



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／ＩＥＣ18033-3:2005（Ｅ）5.2.3.4節に従うこととする。

別記第３　補助関数

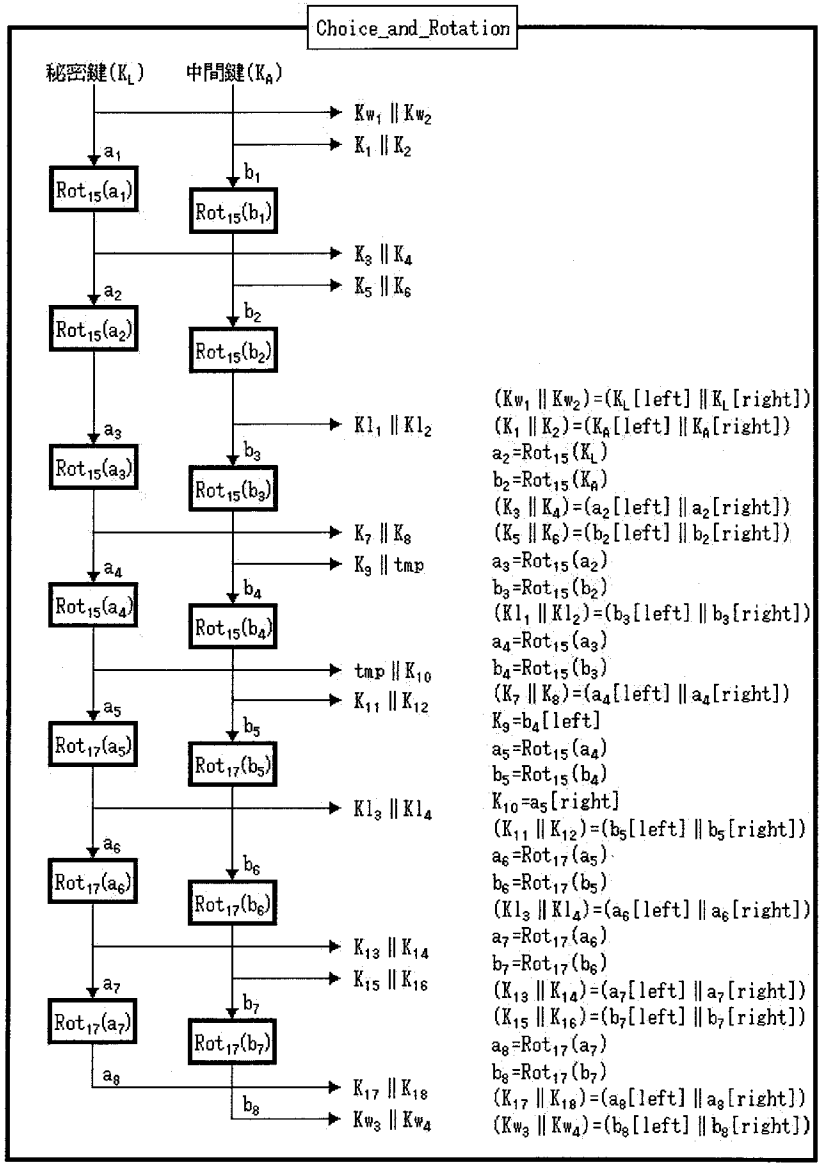


注１　Ｕは、基本関数への入力とする。
２　‖は、ブロックの結合とする。
３　Rot_1は、左巡回１ビットシフトとする。
４　∧は、ビットごとの論理積とする。
５　∨は、ビットごとの論理和とする。
６　Ｕ［left］は、ブロックＵの左32ビットとする。
７　Ｕ［right］は、ブロックＵの右32ビットとする。

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。

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。