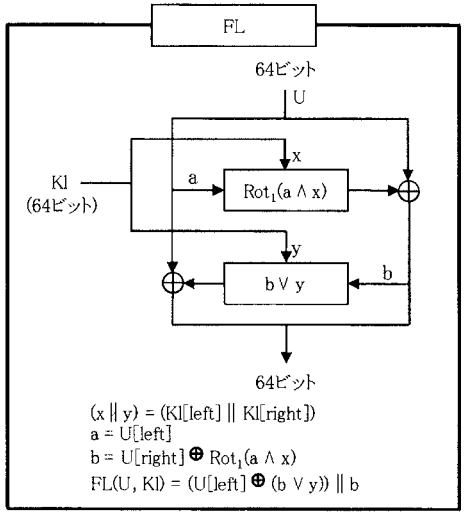
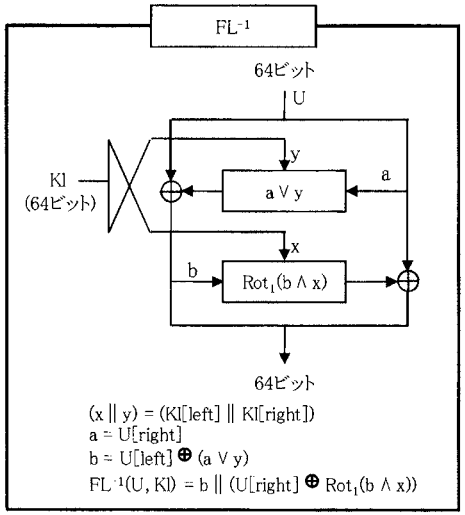
別記第３　補助関数

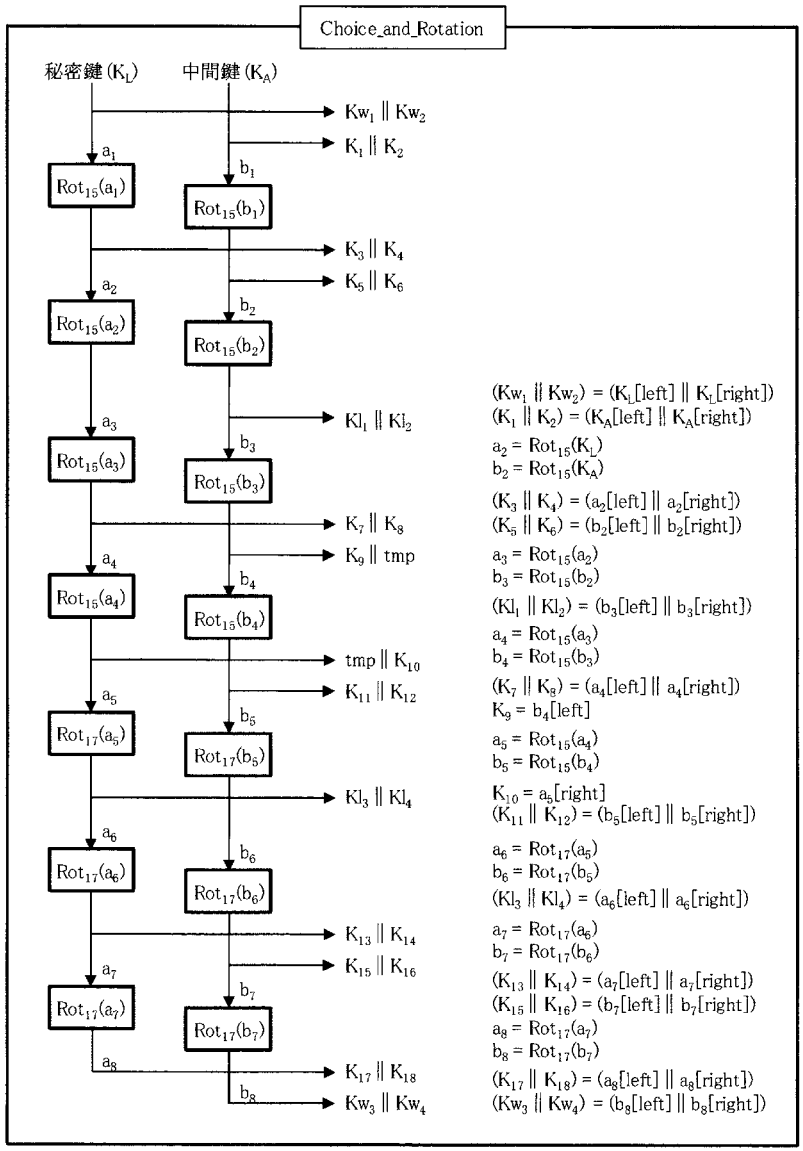




注１　Ｕは、補助関数への入力とする。
　２　‖は、ブロックの結合とする。
　３　Rot_1は、左巡回１ビットシフトとする。
　４　∧は、ビット毎の論理積とする。
　５　∨は、ビット毎の論理和とする。
　６　Ｕ［left］は、ブロックＵの左64ビットとする。
　７　Ｕ［right］は、ブロックＵの右64ビットとする。

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。