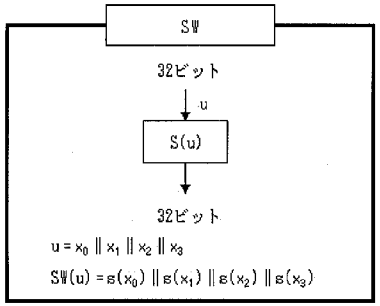
別記第３　アルゴリズム定数

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

注　数値は16進数表記とする。

別記第４　補助関数

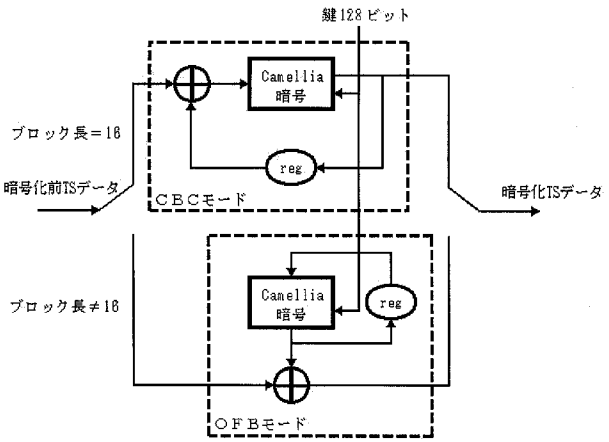


注１　ｕは、補助関数への入力とする。

２　||は、ブロックの結合とする。

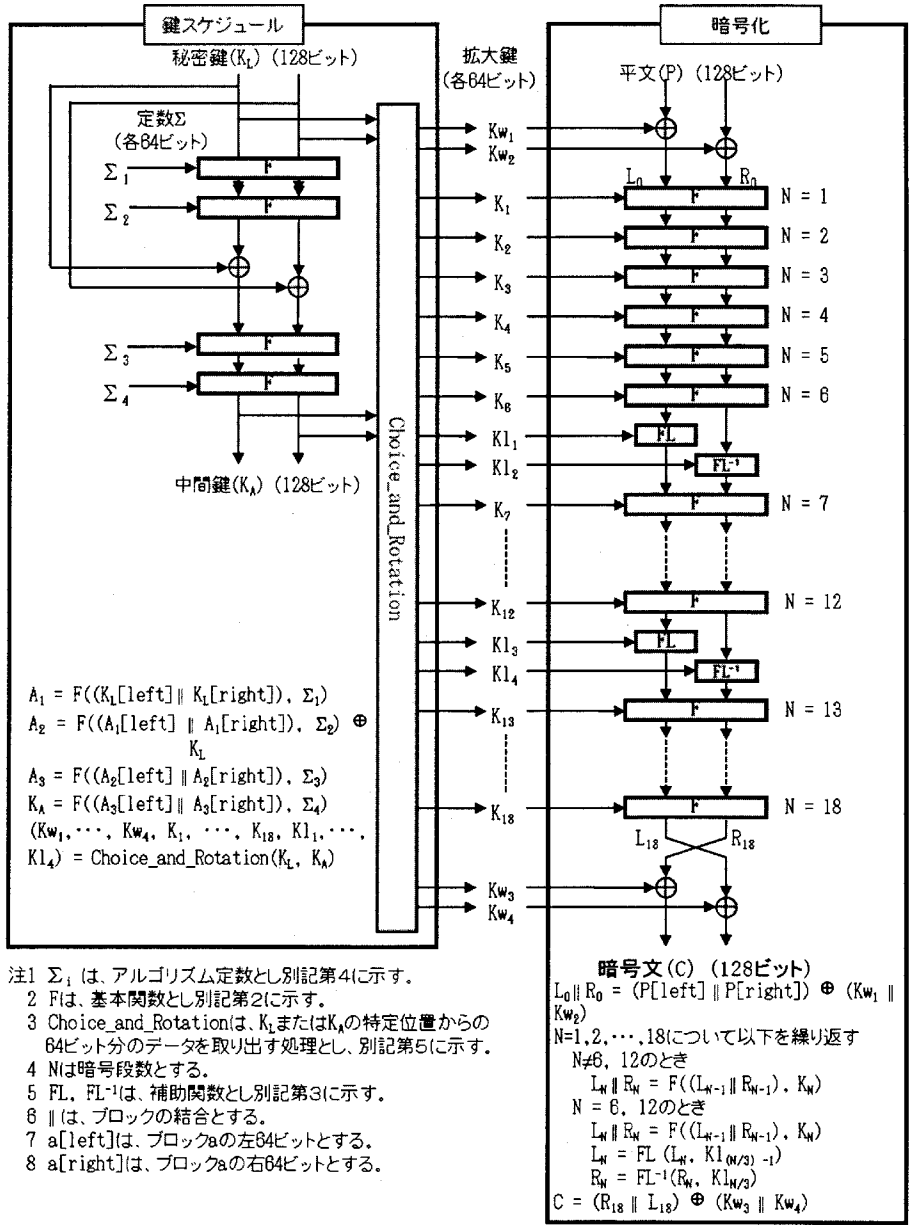
３　ｓは、８ビットの置換表とし、ＩＳＯ／ＩＥＣ18033-3に従うものとする。

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の特定位置からの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。