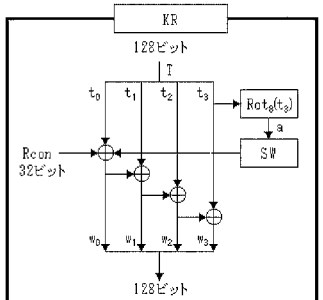
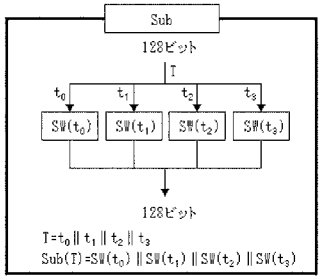
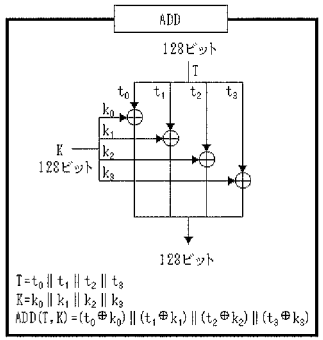
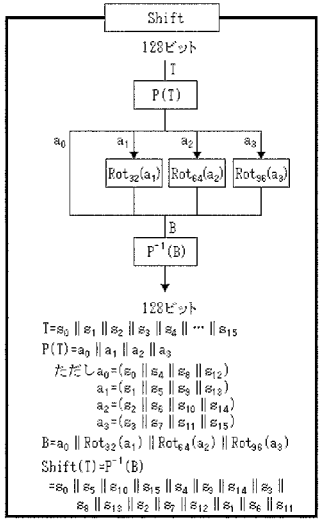
別記第２　基本関数

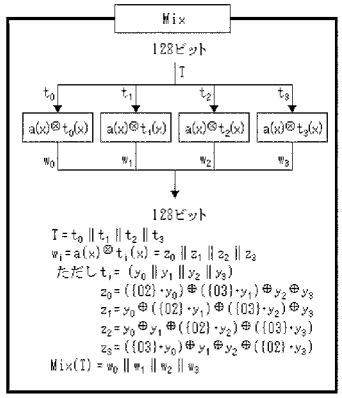








注1　Tは、基本関数への入力とする。
　2　‖は、ブロックの結合とする。
　3　Rot_nは、左巡回nビットシフトとする。
　4　SWは、補助関数とし別記第4に示す。
　5　{}内は、16進数表記とする。
　6　・は、$GF(2^8)$上の乗算を表す。既約多項式は、$x^8+x^4+x^3+x+1$とする。

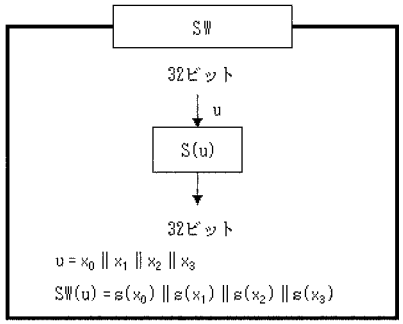


別記第３　アルゴリズム定数

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

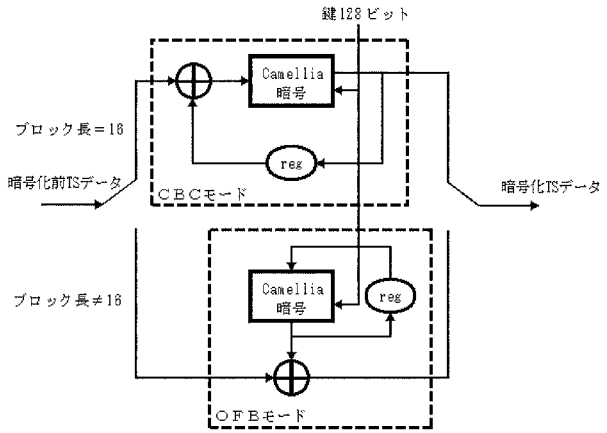
注　数値は16進数表記とする。

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。