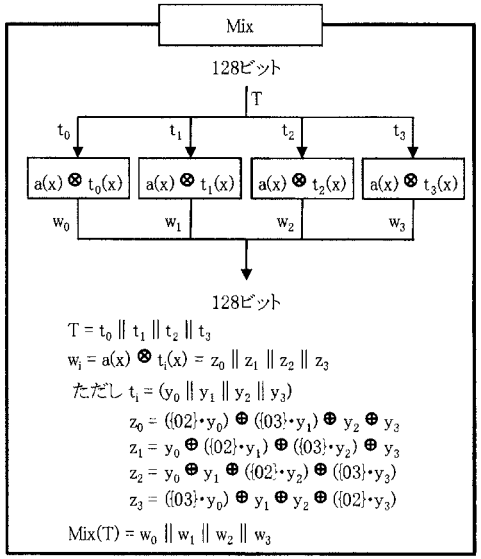
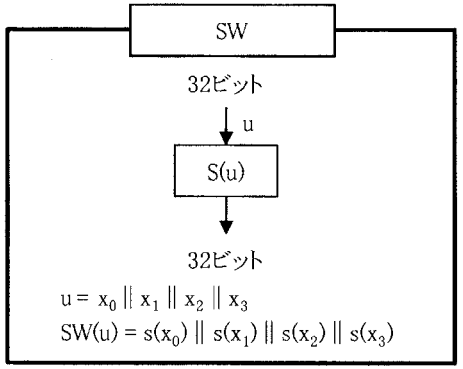
注１　Ｔは、基本関数への入力とする。
　２　‖は、ブロックの結合とする。
　３　Rot_n は、左巡回nビットシフトとする。
　４　SWは、補助関数とし別記第４に示す。
　５　{}内は、16進数表記とする。
　６　・は、GF(2^8)上の乗算を表す。既約多項式は、$x^8 + x^4 + x^3 + x + 1$とする。



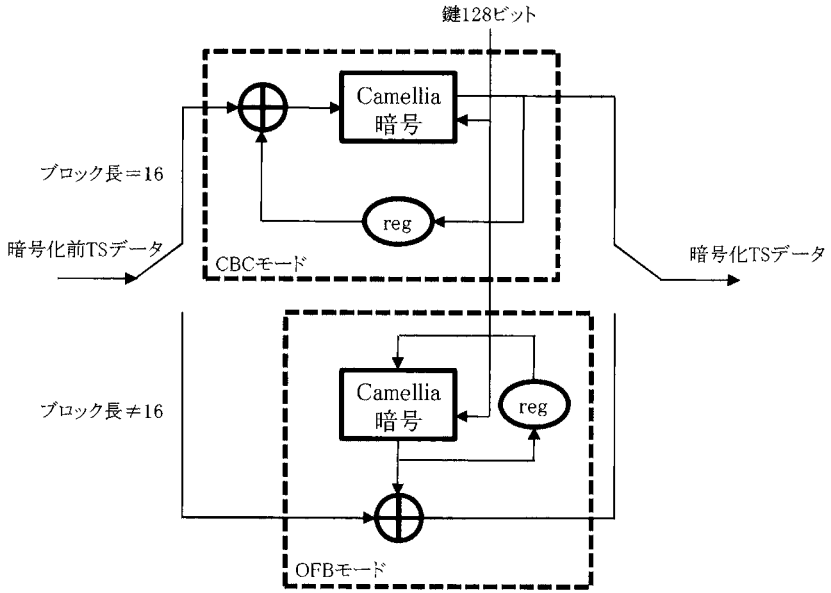
別記第３　アルゴリズム定数
　Rcon［１］＝01000000
　Rcon［２］＝02000000
　Rcon［３］＝04000000
　Rcon［４］＝08000000
　Rcon［５］＝10000000
　Rcon［６］＝20000000
　Rcon［７］＝40000000
　Rcon［８］＝80000000
　Rcon［９］＝1b000000
　Rcon［10］＝36000000
　注　数値は16進数表記とする。

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。