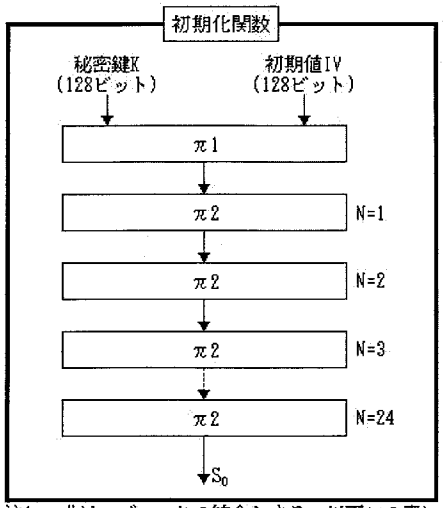
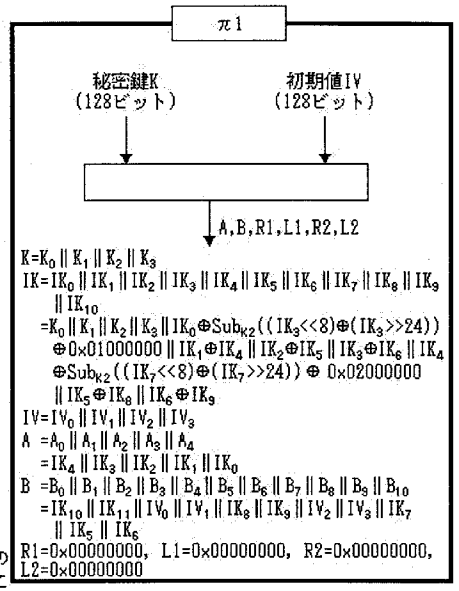
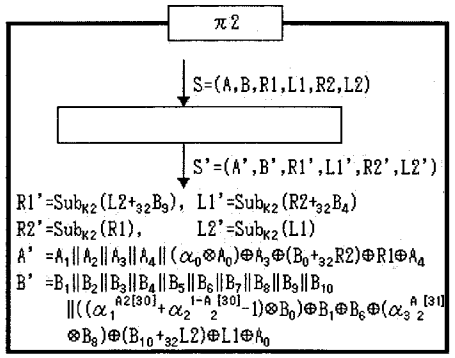
別記第２　初期化関数







注1　‖は、ブロックの結合とする。以下この表において同じ。

2　x<<nは、xのnビット左巡回シフト、x>>nはxのnビット右巡回シフトを示すものとする。以下この表において同じ。

3　A_0からA_4まで、B_0からB_{10}まで、R1、L1、R2及びL2は32ビットの値を示す変数とする。

4　「0x」に続く数字を16進数とする。以下この表において同じ。

5　$+_{32}$及び⊗は、それぞれGF(2^{32})上の算術加算と乗算を示すものとする。以下この表において同じ。

6　Sub_{K2}は、別表第2号に示すSW関数・Mix関数を順に適用する関数とする。以下この表において同じ。

7　α_0は、GF(2^{32})上の元であり、$x^4+\beta^{24}x^3+\beta^3x^2+\beta^{12}x+\beta^{71} \in GF(2^8)[x]$の根とする。ただし、$\beta$は原始多項式$x^8+x^7+x^6+x+1 \in GF(2)[x]$の根とする。以下この表において同じ。

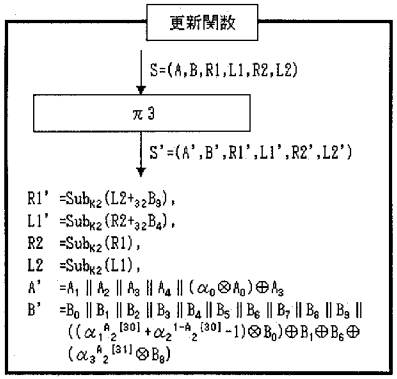
8　α_1はGF(2^{32})上の元であり$x^4+\gamma^{230}x^3+\gamma^{156}x^2+\gamma^{93}x+\gamma^{29} \in GF(2^8)[x]$の根とする。ただし、$\gamma$は原始多項式$x^8+x^5+x^3+x^2+1 \in GF(2)[x]$の根とする。以下この表において同じ。

9　X[Y]は、XのY番目のビットを示すものとする。以下この表において同じ。

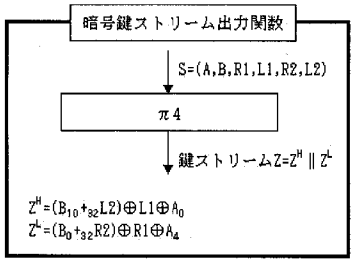
10　α_2はGF(2^{32})上の元であり$x^4+\delta^{34}x^3+\delta^{16}x^2+\delta^{199}x+\delta^{248} \in GF(2^8)[x]$の根とする。ただし、$\delta$は原始多項式$x^8+x^6+x^3+x^2+1 \in GF(2)[x]$の根とする。以下この表において同じ。

11　α_3はGF(2^{32})上の元であり$x^4+\xi^{157}x^3+\xi^{253}x^2+\xi^{56}x+\xi^{16} \in GF(2^8)[x]$の根とする。ただし、$\xi$は原始多項式$x^8+x^6+x^5+x^2+1 \in GF(2)[x]$の根とする。以下この表において同じ。

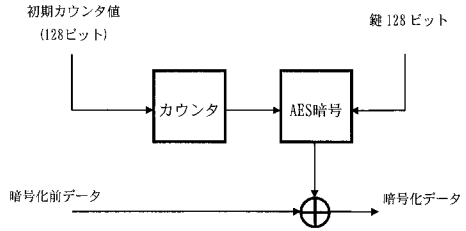
別記第３　更新関数



別記第４　暗号鍵ストリーム出力関数

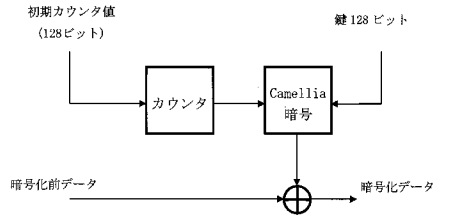


別表第八号



注　ＡＥＳ暗号は、別表第二号別記第１に示す。

別表第九号



注　Camellia暗号は、別表第三号別記第１に示す。