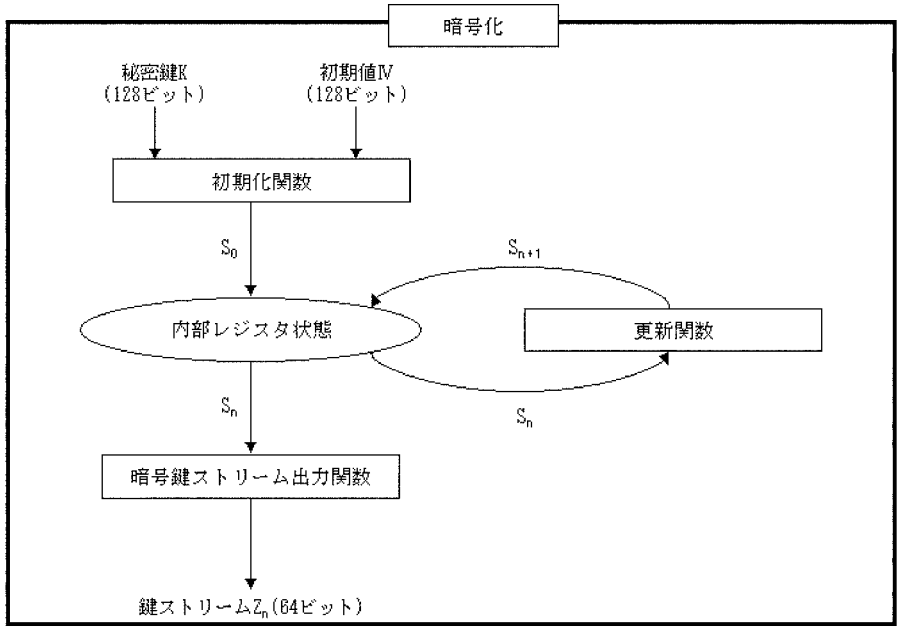
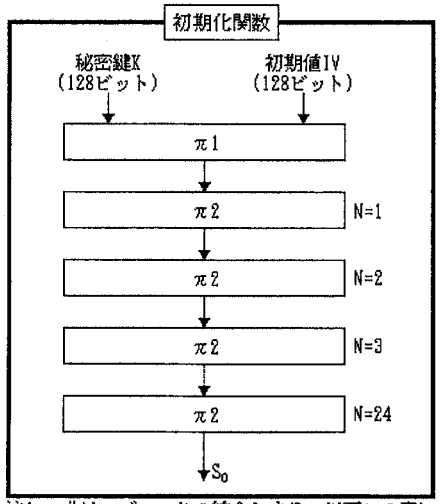
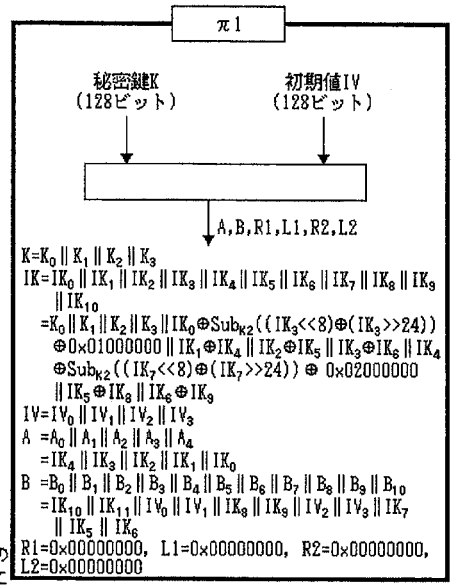
別記第１　KCipher―2暗号

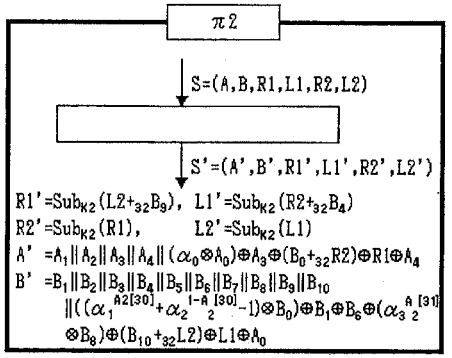


注１　初期化関数は、別記第２に示す。
　２　S_nは内部レジスタ状態を示すものとする。
　３　更新関数は、別記第３に示す。
　４　暗号鍵ストリーム出力関数は、別記第４に示す。

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、$\chi^4+\beta^{24}\chi^3+\beta^3\chi^2+\beta^{12}\chi+\beta^{71}\in GF(2^8)[\chi]$の根とする。ただし、$\beta$は原始多項式$\chi^8+\chi^7+\chi^6+\chi+1\in GF(2)[\chi]$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$\chi^4+\gamma^{230}\chi^3+\gamma^{156}\chi^2+\gamma^{93}\chi+\gamma^{29}\in GF(2^8)[\chi]$の根とする。ただし、$\gamma$は原始多項式$\chi^8+\chi^5+\chi^3+\chi^2+1\in GF(2)[\chi]$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$\chi^4+\delta^{34}\chi^3+\delta^{16}\chi^2+\delta^{199}\chi+\delta^{248}\in GF(2^8)[\chi]$の根とする。ただし、$\delta$は原始多項式$\chi^8+\chi^6+\chi^3+\chi^2+1\in GF(2)[\chi]$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$\chi^4+\xi^{157}\chi^3+\xi^{253}\chi^2+\xi^{56}\chi+\xi^{16}\in GF(2^8)[\chi]$の根とする。ただし、$\xi$は原始多項式$\chi^8+\chi^6+\chi^5+\chi^2+1\in GF(2)[\chi]$の根とする。以下この表において同じ。