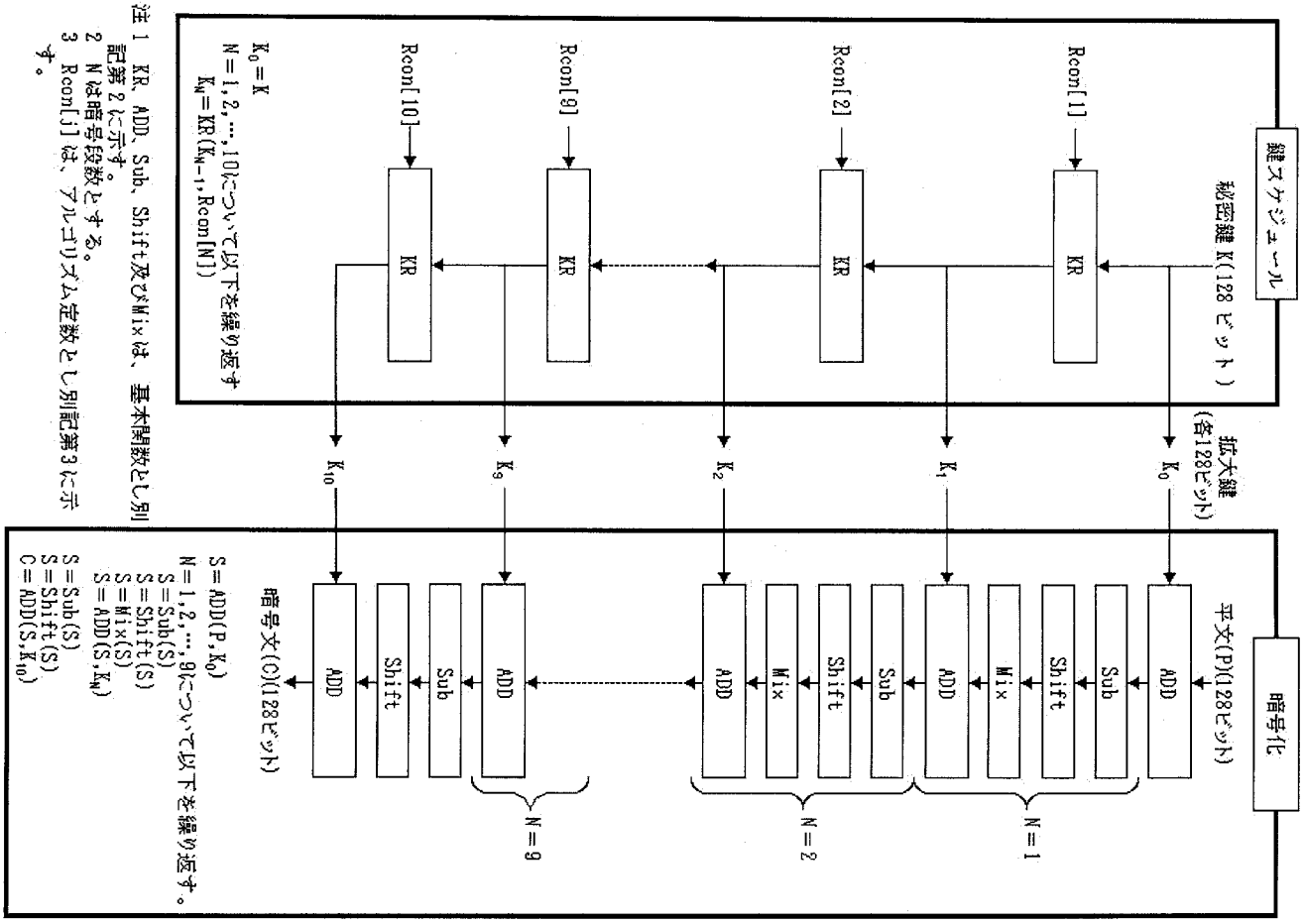
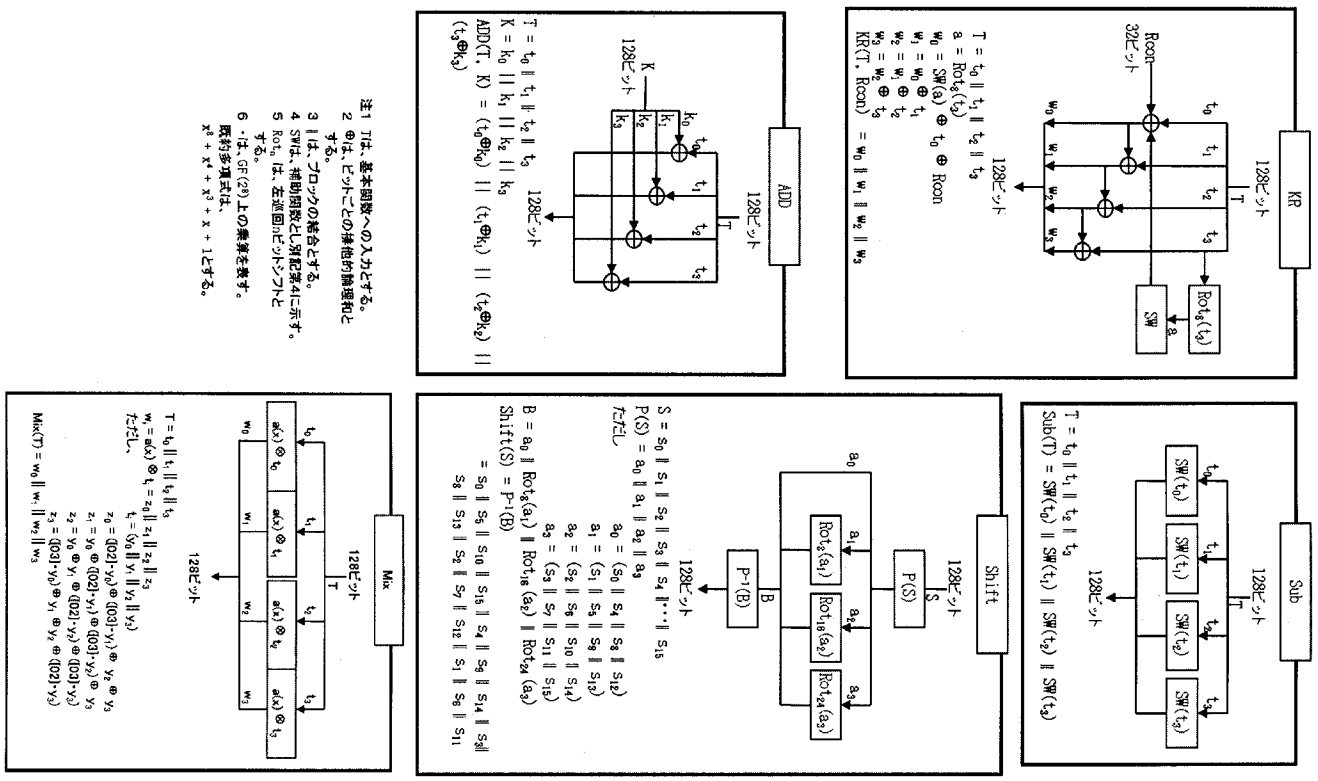
別記第1　ＡＥＳ暗号



注 1　KR、ADD、Sub、Shift及びMixは、基本関数とし別記第２に示す。
2　Ｎは暗号段数とする。
3　Rcon[j]は、アルゴリズム定数とし別記第３に示す。

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、ビットごとの排他的論理和とする。
3　‖は、ブロックの結合とする。
4　SWは、補助関数とし別記第4に示す。
5　Rot_nは、左巡回nビットシフトとする。
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。