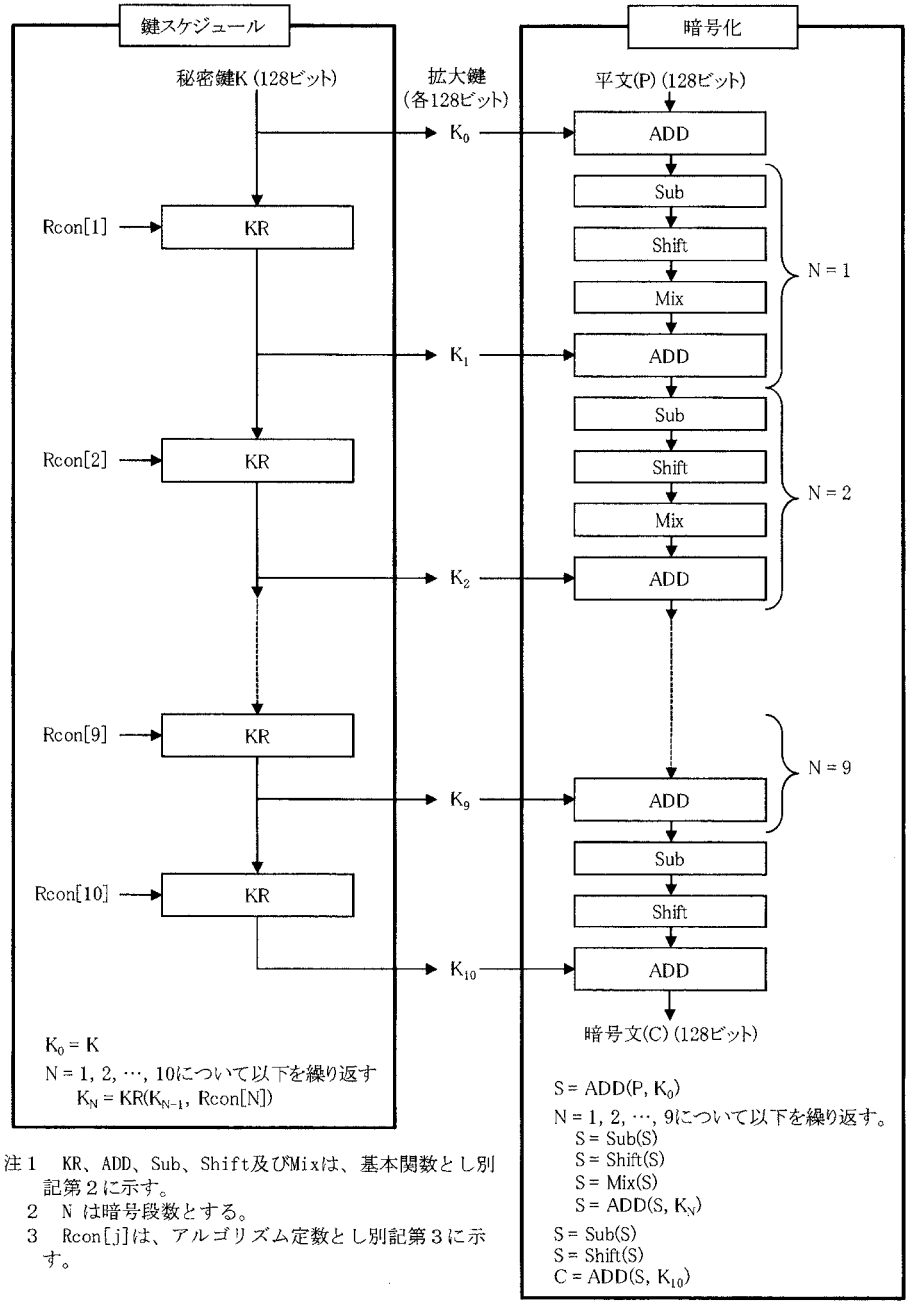
別記第１　AES暗号



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

