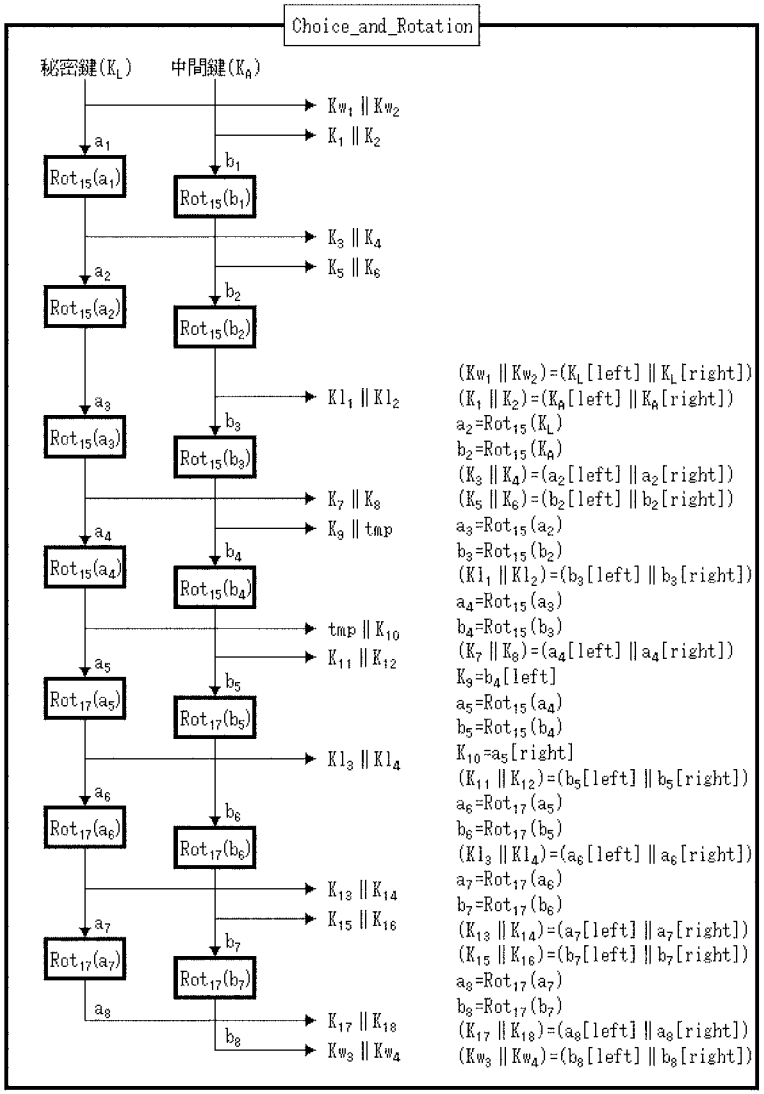
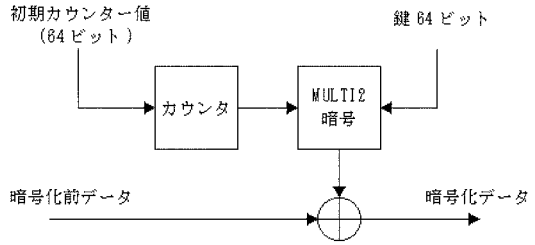
別記第５　Choice_and_Rotation



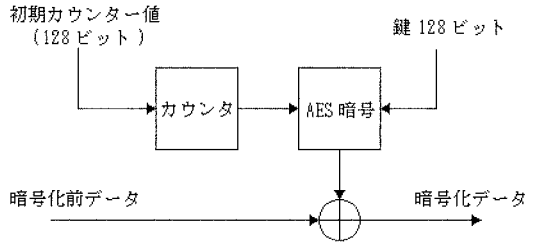
注１　Rot_nは、左巡回ｎビットシフトとする。
　２　‖は、ブロックの結合とする。
　３　Ｕ［left］は、ブロックＵの左64ビットとする。
　４　Ｕ［right］は、ブロックＵの右64ビットとする。

別表第四号



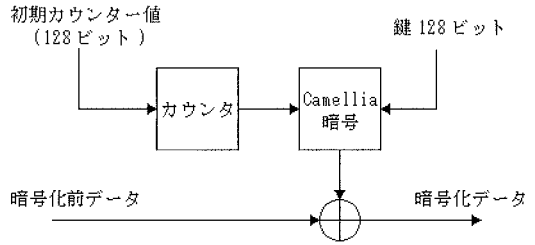
注　ＭＵＬＴＩ２暗号は、別表第一号別記第１に示す。

別表第五号



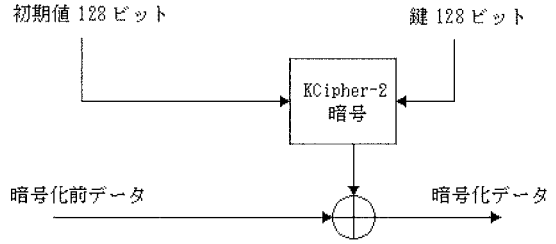
注　ＡＥＳ暗号は、別表第二号別記第１に示す。

別表第六号



注　Camellia暗号は、別表第三号別記第１に示す。

別表第七号



注　KChipher―２暗号は、別記第１に示す。