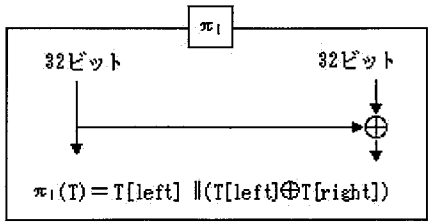
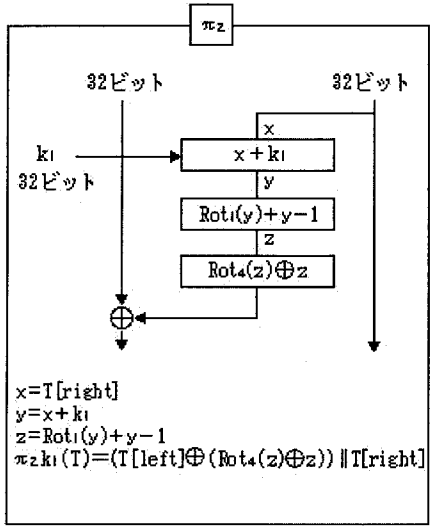
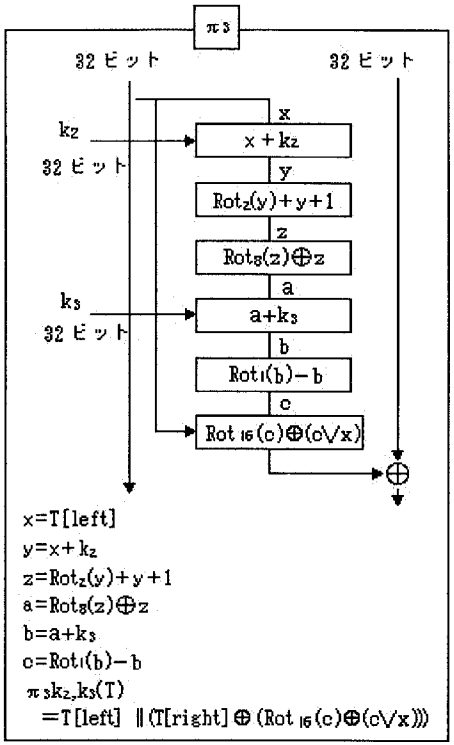
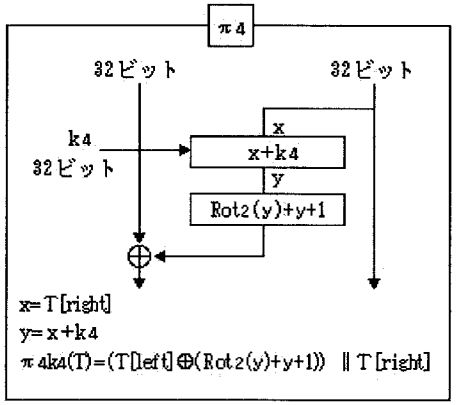
別記第２　基本関数



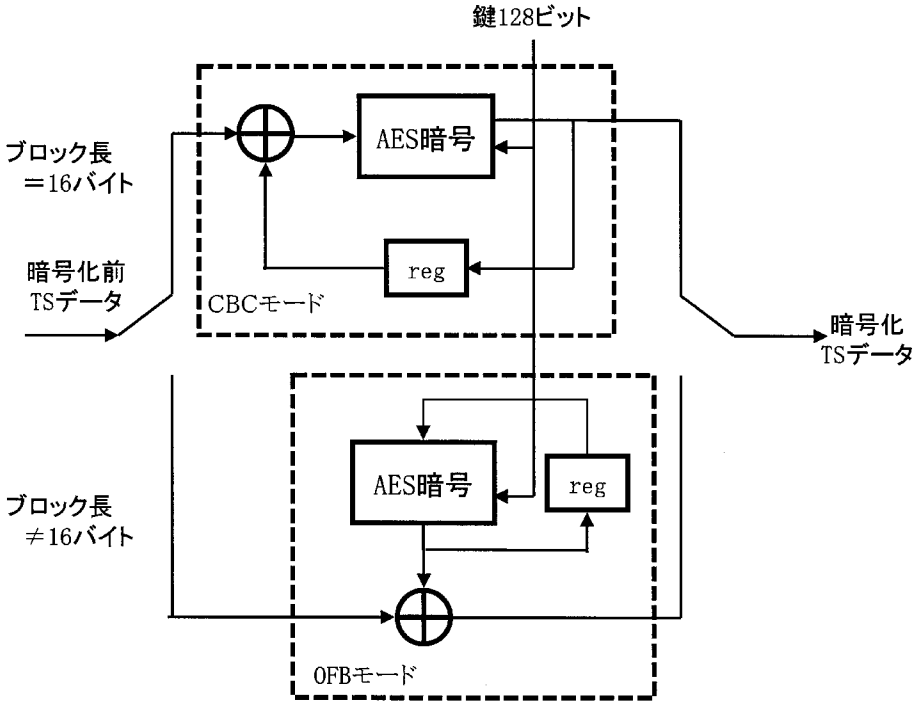






注１　Tは、基本関数への入力とする。
２　T[left]は、ブロックTの左32ビットとする。
３　T[right]は、ブロックTの右32ビットとする。
４　＋は、2^{32}を法とした加算とする。
５　－は、2^{32}を法とした減算とする。
６　Rotsは、左巡回sビットシフトとする。
７　∨は、ビット毎の論理和とする。
８　‖は、ブロックの結合とする。

別表第二号



注　ＡＥＳ暗号は、別記第１に示す。