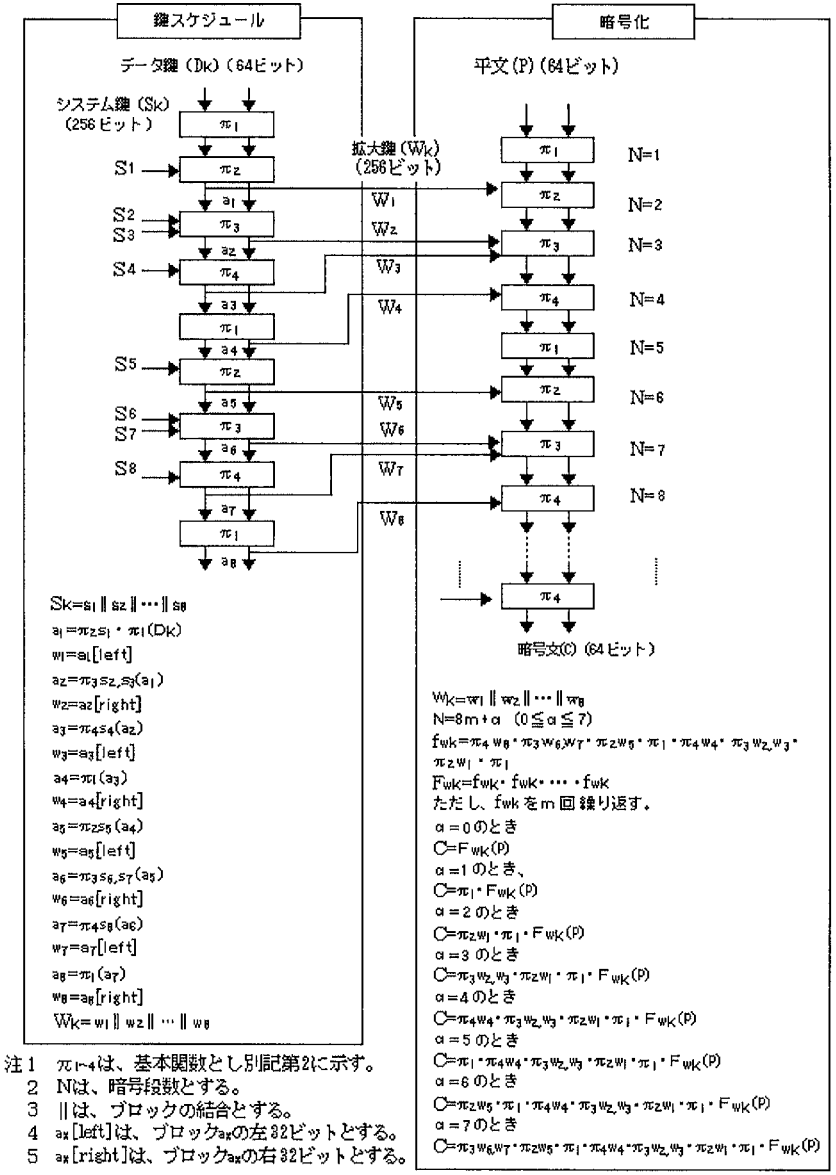
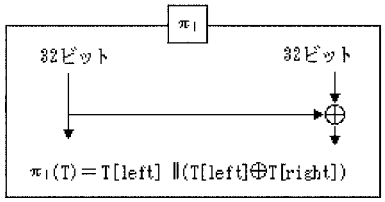
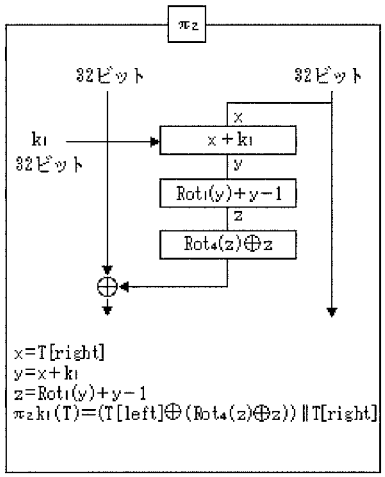
別記第１　ＭＵＬＴＩ２暗号

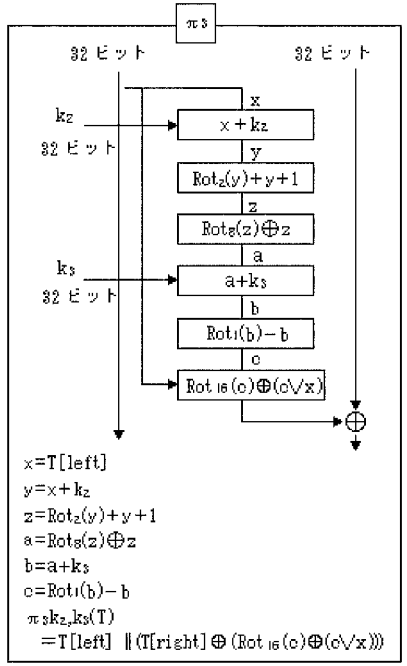


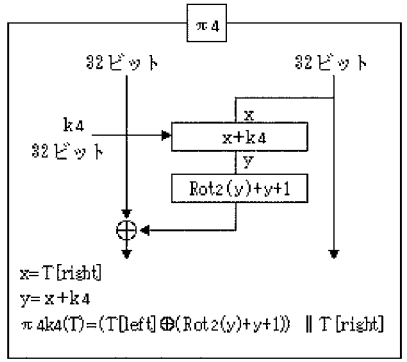
注１　πi-4は、基本関数とし別記第2に示す。
　２　Nは、暗号段数とする。
　３　‖は、ブロックの結合とする。
　４　ax[left]は、ブロックaxの左32ビットとする。
　５　ax[right]は、ブロックaxの右32ビットとする。

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。