S-AES

key schedule

user supplied key

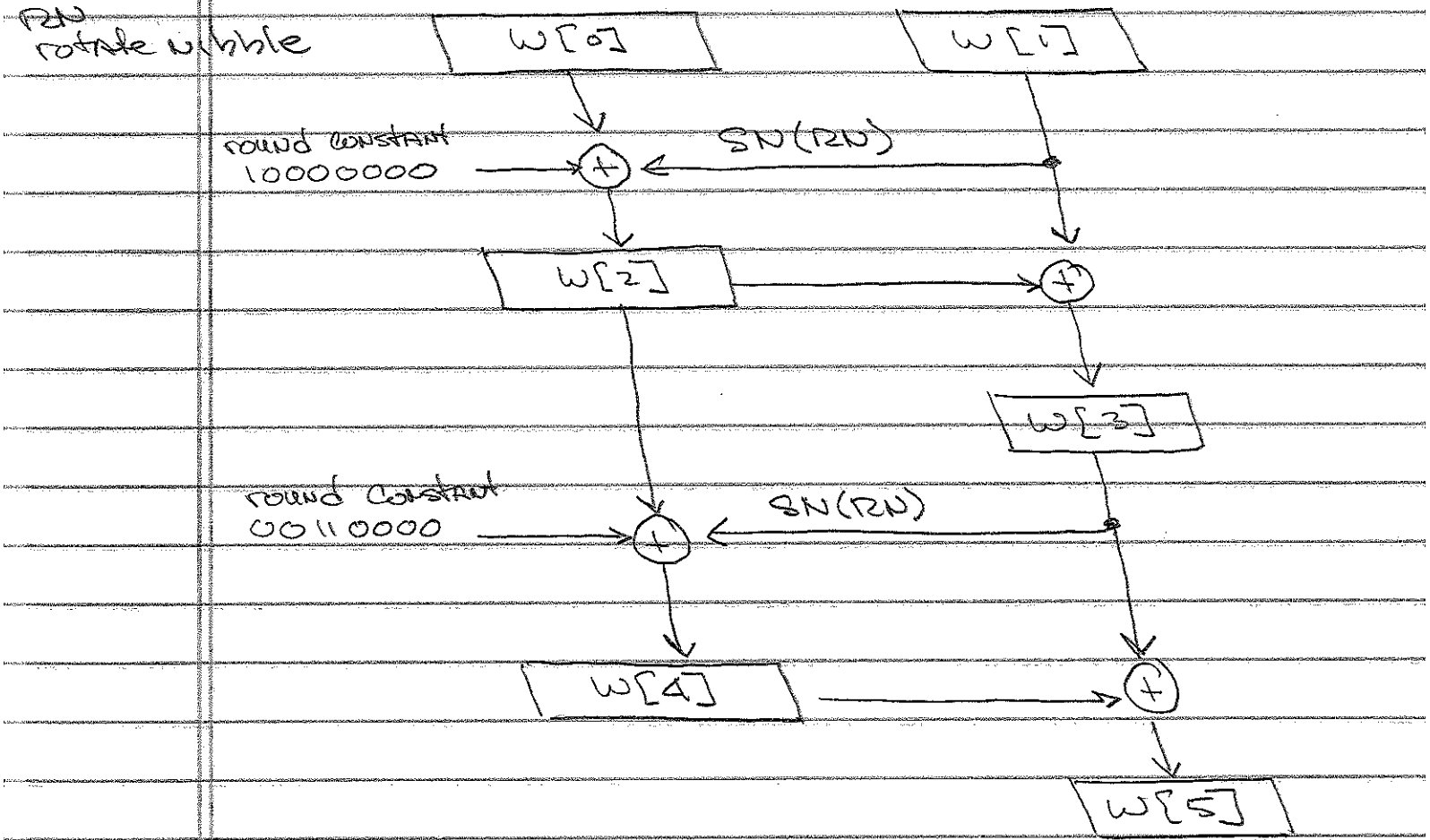
16 bits

$k_0 k_1 k_2 k_3 \quad k_4 k_5 k_6 k_7 \quad k_8 k_9 k_{10} k_{11} \quad k_{12} k_{13} k_{14} k_{15}$

$w[0]$ $\quad$ $w[1]$

SN substitute nibble

RN rotate nibble



K_0 $\quad w[0]\,w[1]$

K_1 $\quad w[2]\,w[3]$

K_2 $\quad w[4]\,w[5]$

user supplied key

1010 0111 | 0011 1011

w[0] | w[1]

w[0] = 1010 0111

w[1] = 0011 1011

RN

1011 0011

SN

0011 1011

⊕ round constant 1000 0000

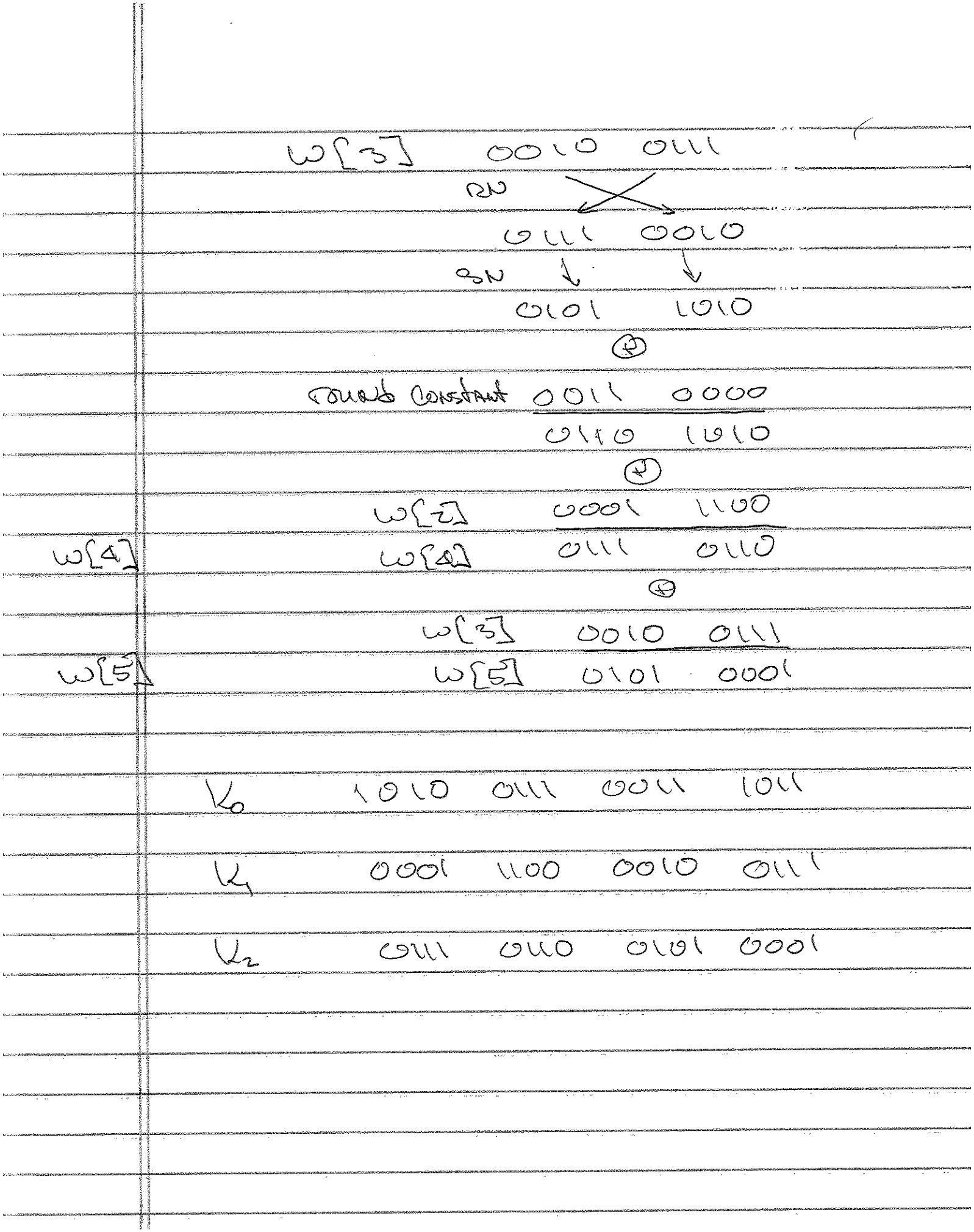
1011 1011

⊕ w[0] 1010 0111

w[2] = 0001 1100

⊕ w[1] 0011 1011

w[3] = 0010 0111


w[3] 0010 0111
RN
0111 0010
SN
0101 1010
⊕
Round Constant 0011 0000
0110 1010
⊕
w[4] w[2] 0001 1100
0111 0110
⊕
w[5] w[3] 0010 0111
w[5] 0101 0001
K0 1010 0111 0011 1011
K1 0001 1100 0010 0111
K2 0111 0110 0101 0001