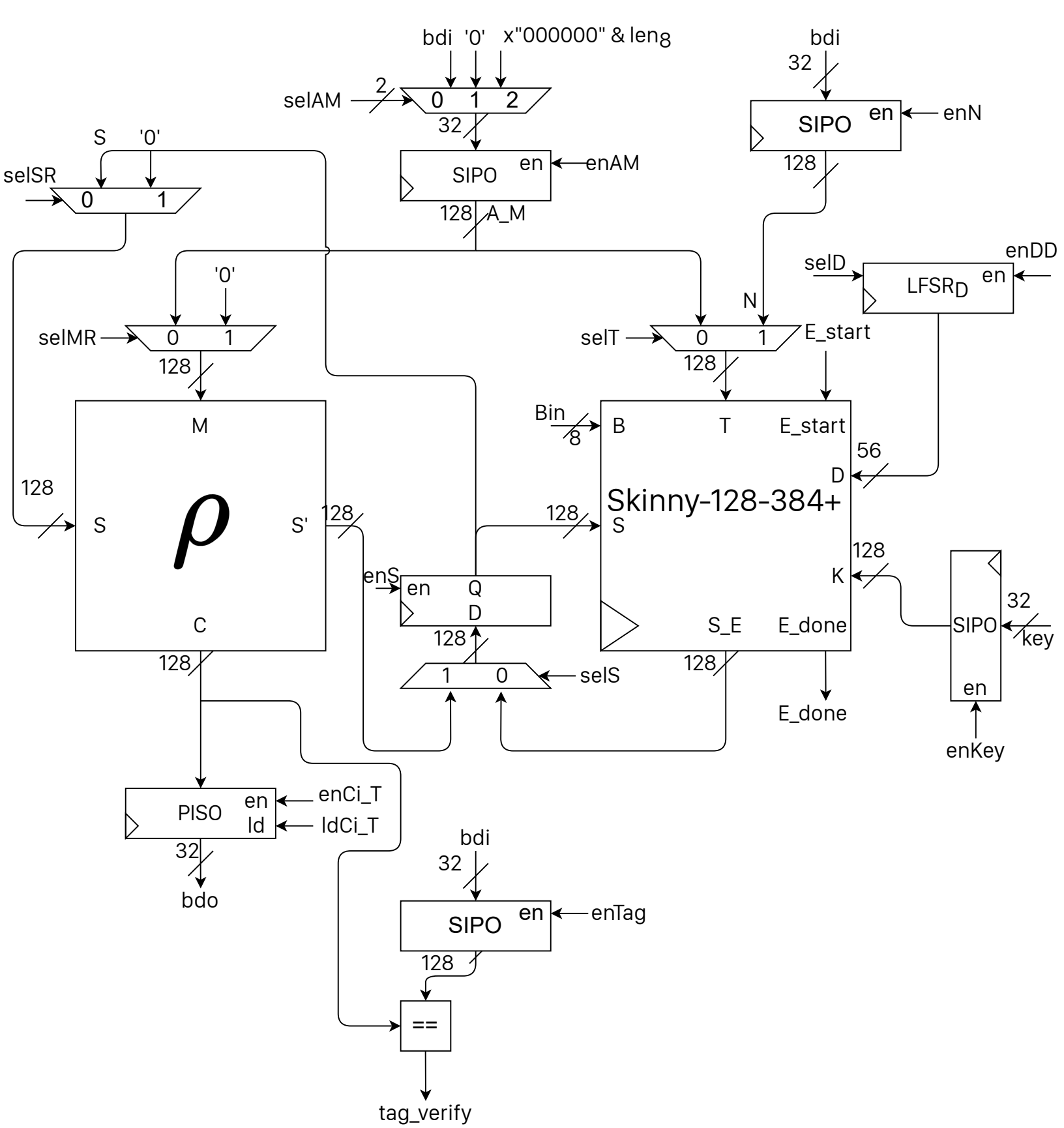
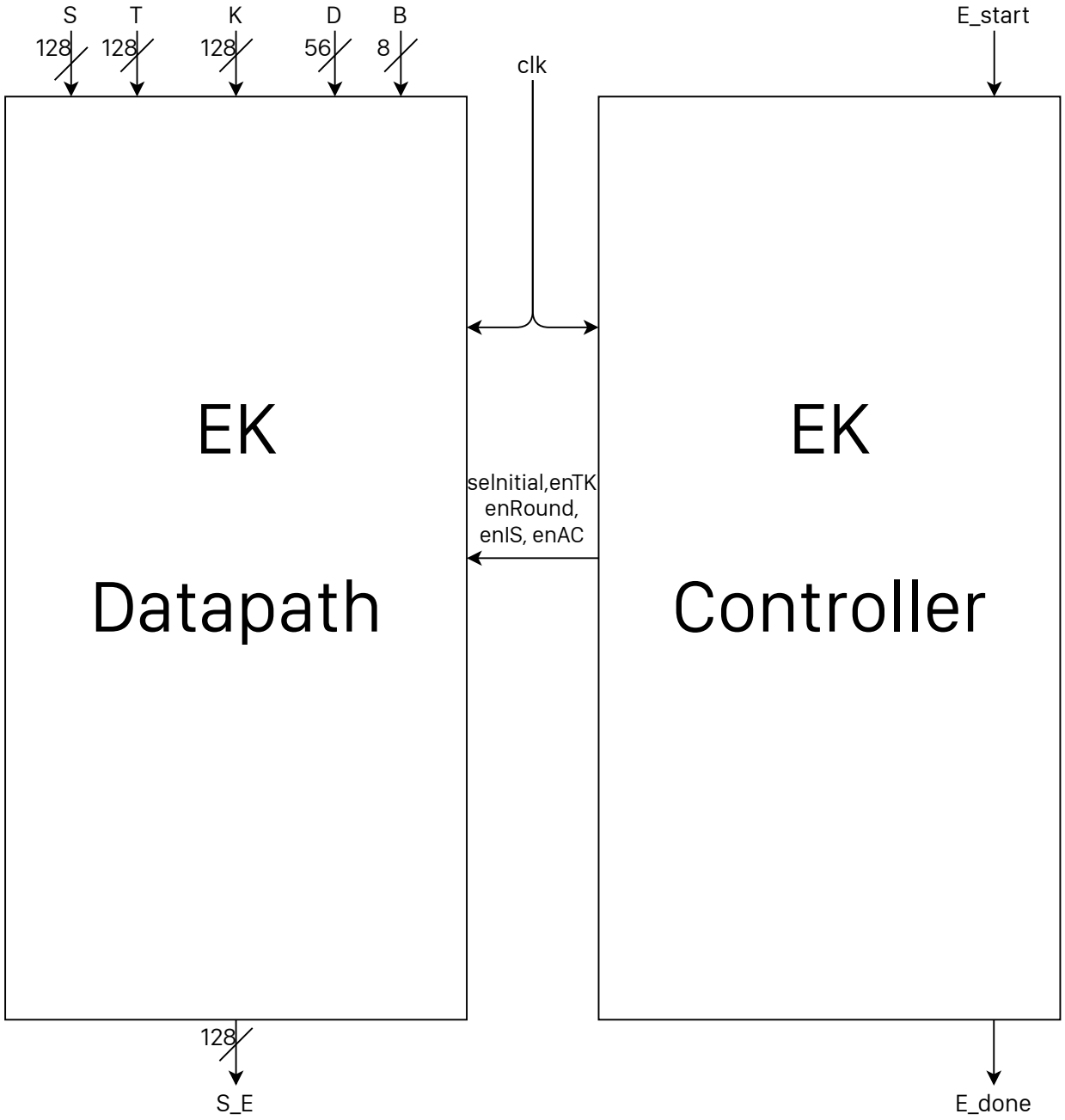
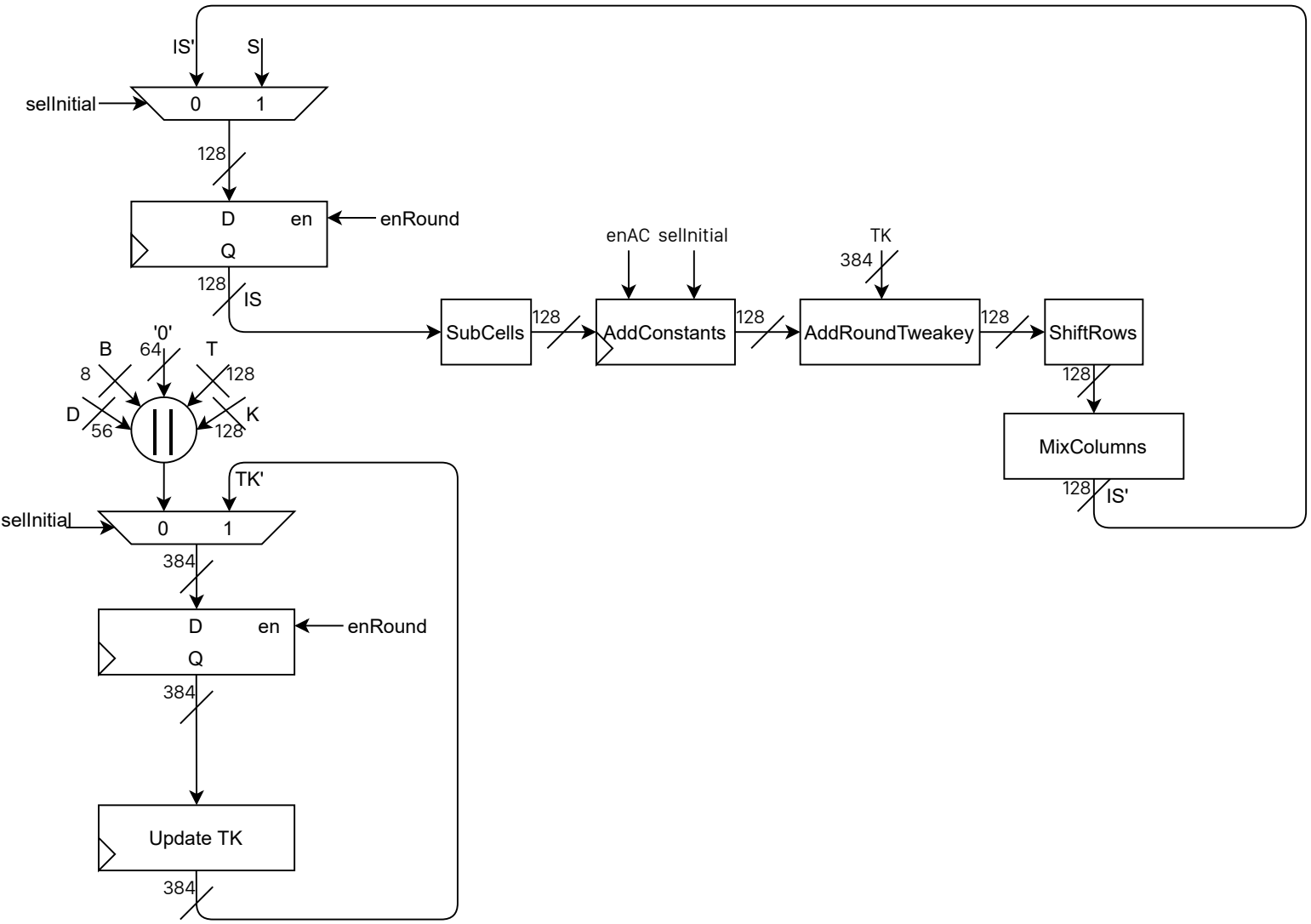
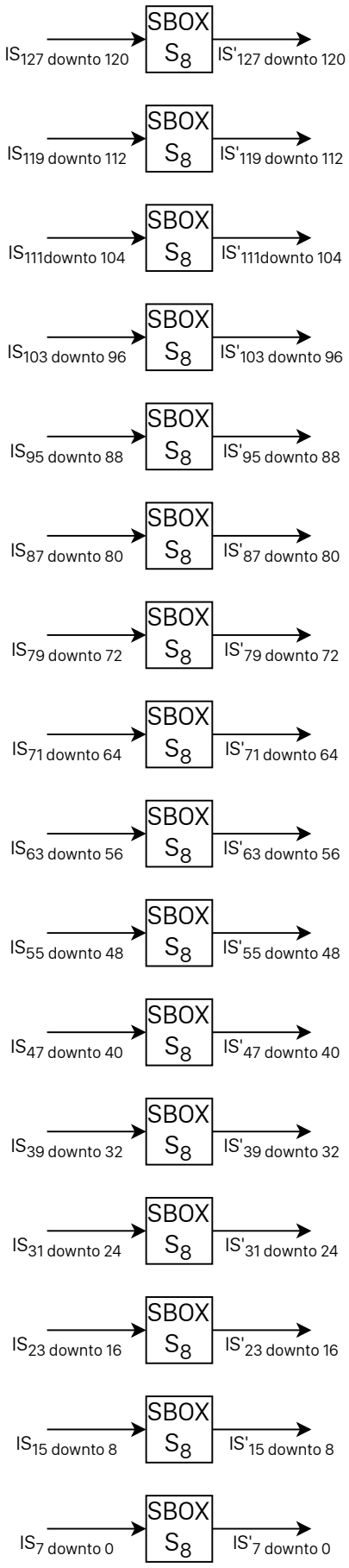

bdi
'0'
x"000000" & len8
selAM
2
0 1 2
32
SIPO
en
enAM
128
A_M
bdi
32
SIPO
en
enN
128
S
'0'
selSR
0 1
'0'
selMR
0 1
128
M
ρ
S
S'
C
128
128
128
enS
en
Q
D
128
1 0
selS
selT
0 1
128
N
E_start
selD
LFSR_D
en
enDD
Bin
8
B
T
E_start
Skinny-128-384+
S
D
56
K
128
S_E
E_done
128
E_done
SIPO
en
32
key
enKey
PISO
en
ld
enCi_T
ldCi_T
32
bdo
bdi
32
SIPO
en
enTag
128
==
tag_verify


S
128
T
128
K
128
D
56
B
8
clk
E_start
EK
Datapath
selnitial,enTK
enRound,
enIS, enAC
EK
Controller
128
S_E
E_done

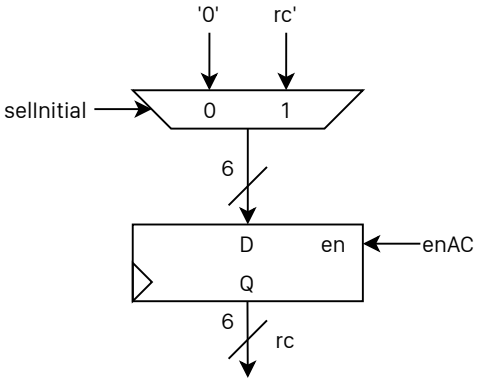
E_K Top Level Datapath

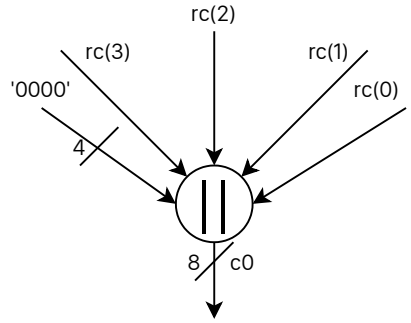


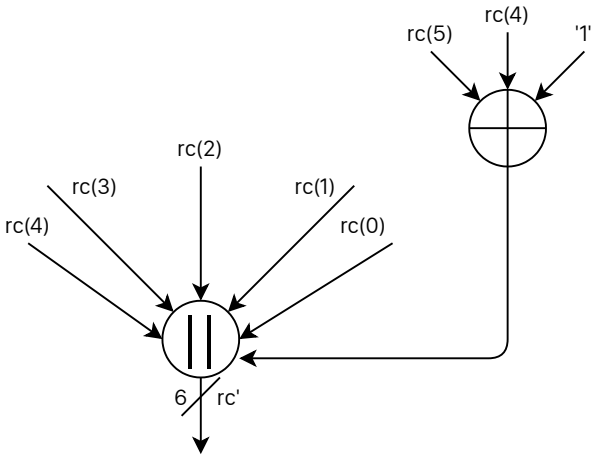
SubCells

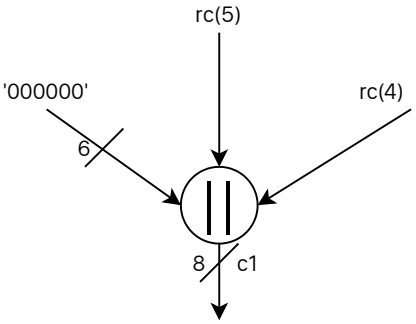

IS127 downto 120
SBOX S8
IS'127 downto 120
IS119 downto 112
SBOX S8
IS'119 downto 112
IS111downto 104
SBOX S8
IS'111downto 104
IS103 downto 96
SBOX S8
IS'103 downto 96
IS95 downto 88
SBOX S8
IS'95 downto 88
IS87 downto 80
SBOX S8
IS'87 downto 80
IS79 downto 72
SBOX S8
IS'79 downto 72
IS71 downto 64
SBOX S8
IS'71 downto 64
IS63 downto 56
SBOX S8
IS'63 downto 56
IS55 downto 48
SBOX S8
IS'55 downto 48
IS47 downto 40
SBOX S8
IS'47 downto 40
IS39 downto 32
SBOX S8
IS'39 downto 32
IS31 downto 24
SBOX S8
IS'31 downto 24
IS23 downto 16
SBOX S8
IS'23 downto 16
IS15 downto 8
SBOX S8
IS'15 downto 8
IS7 downto 0
SBOX S8
IS'7 downto 0

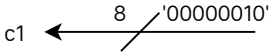
AddConstants

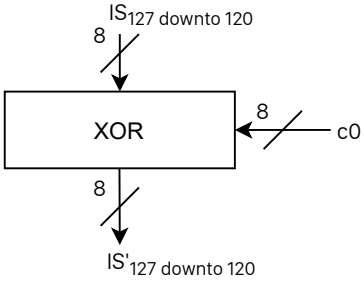


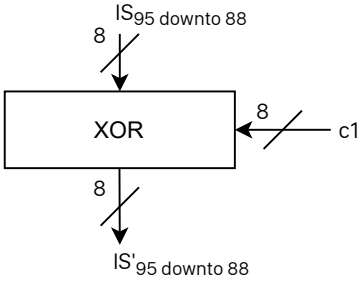


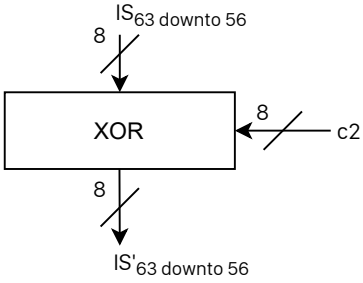


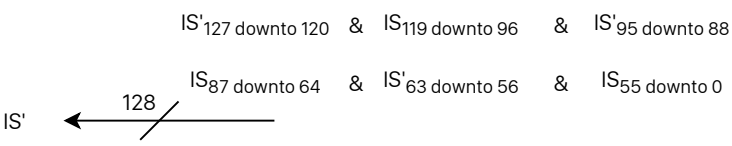




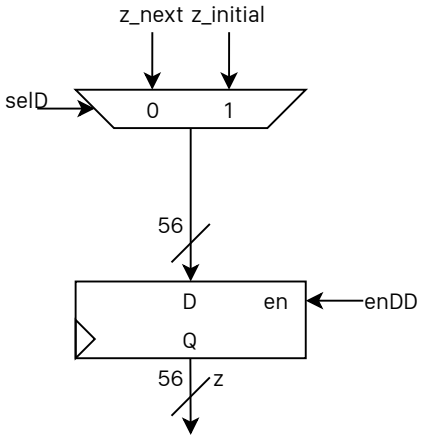








$LFSR_D$

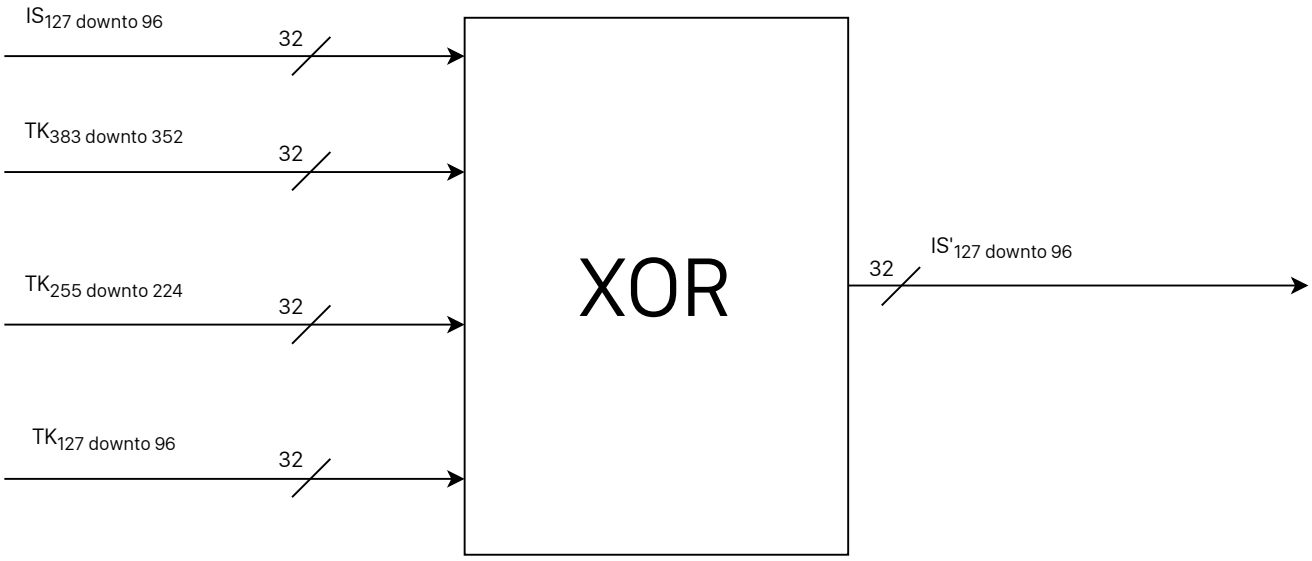


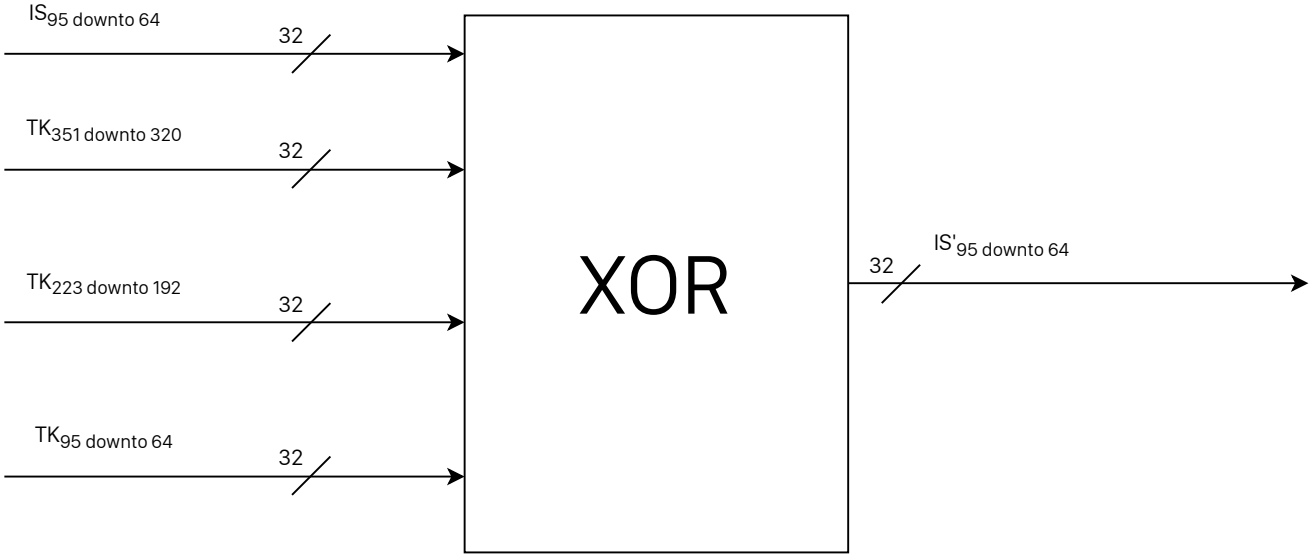
z_initial ← 56 '00000001' & (others => '0')

z_next ← 56 $Z_{54\ downto\ 7}$ & Z_6 XOR Z_{55} & Z_3 XOR Z_{55} & Z_1 XOR Z_{55} & Z_{55}

AddRoundTweakey

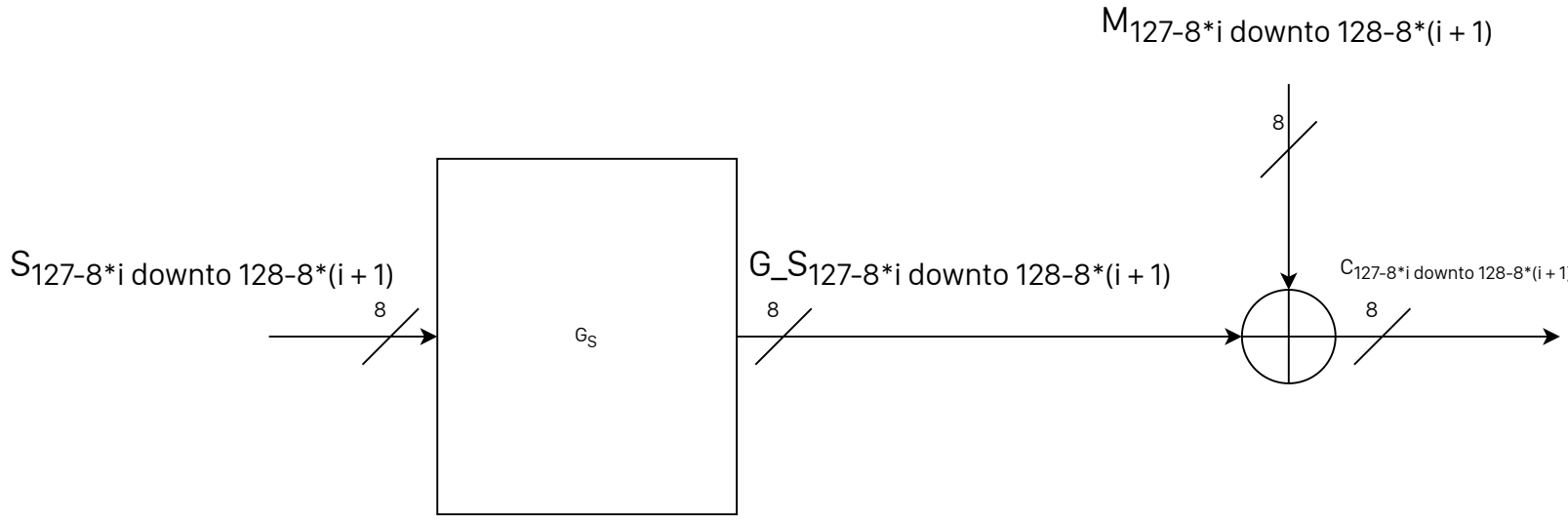
$IS'_{63\ downto\ 0}$ ← 64 $IS_{63\ downto\ 0}$

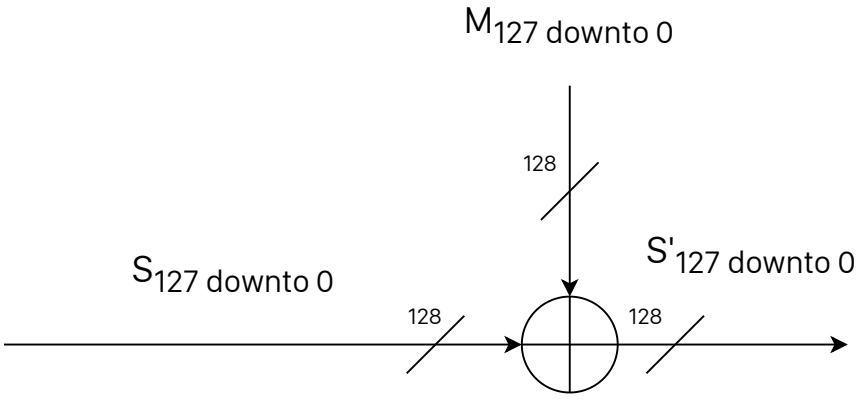




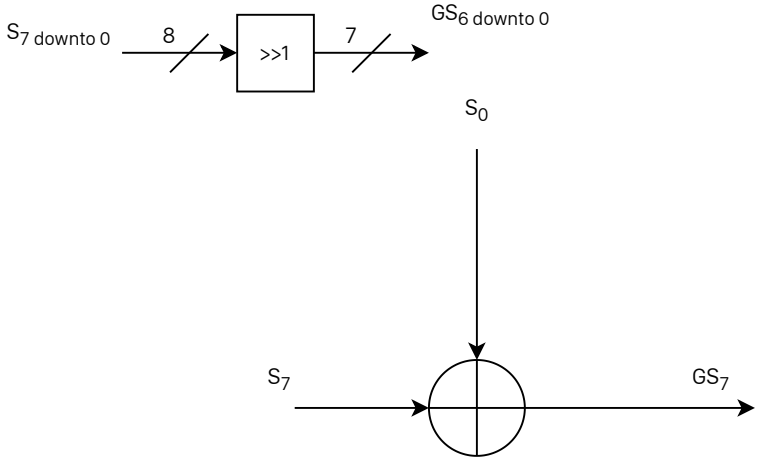
Rho Function

for i in 0 to 15 generate



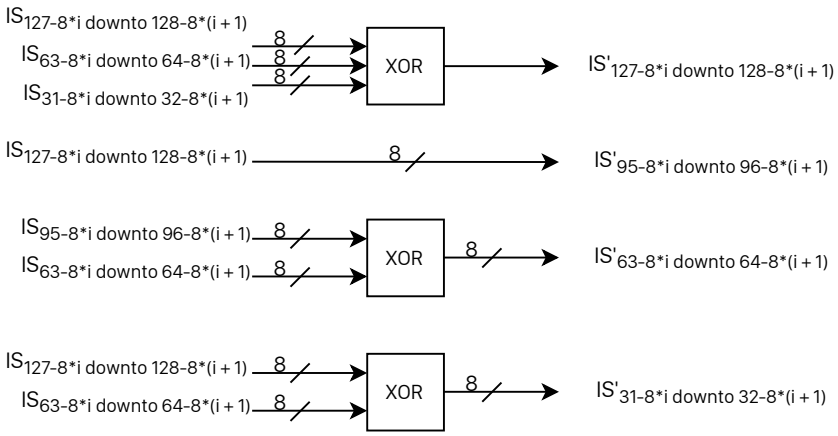
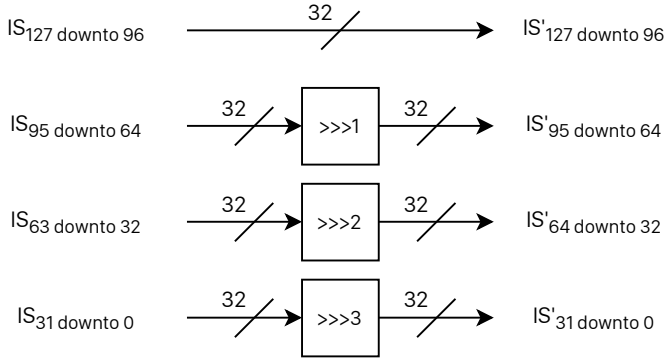


G_s Function



MixColumns

for i in 0 to 3 generate



ShiftRows