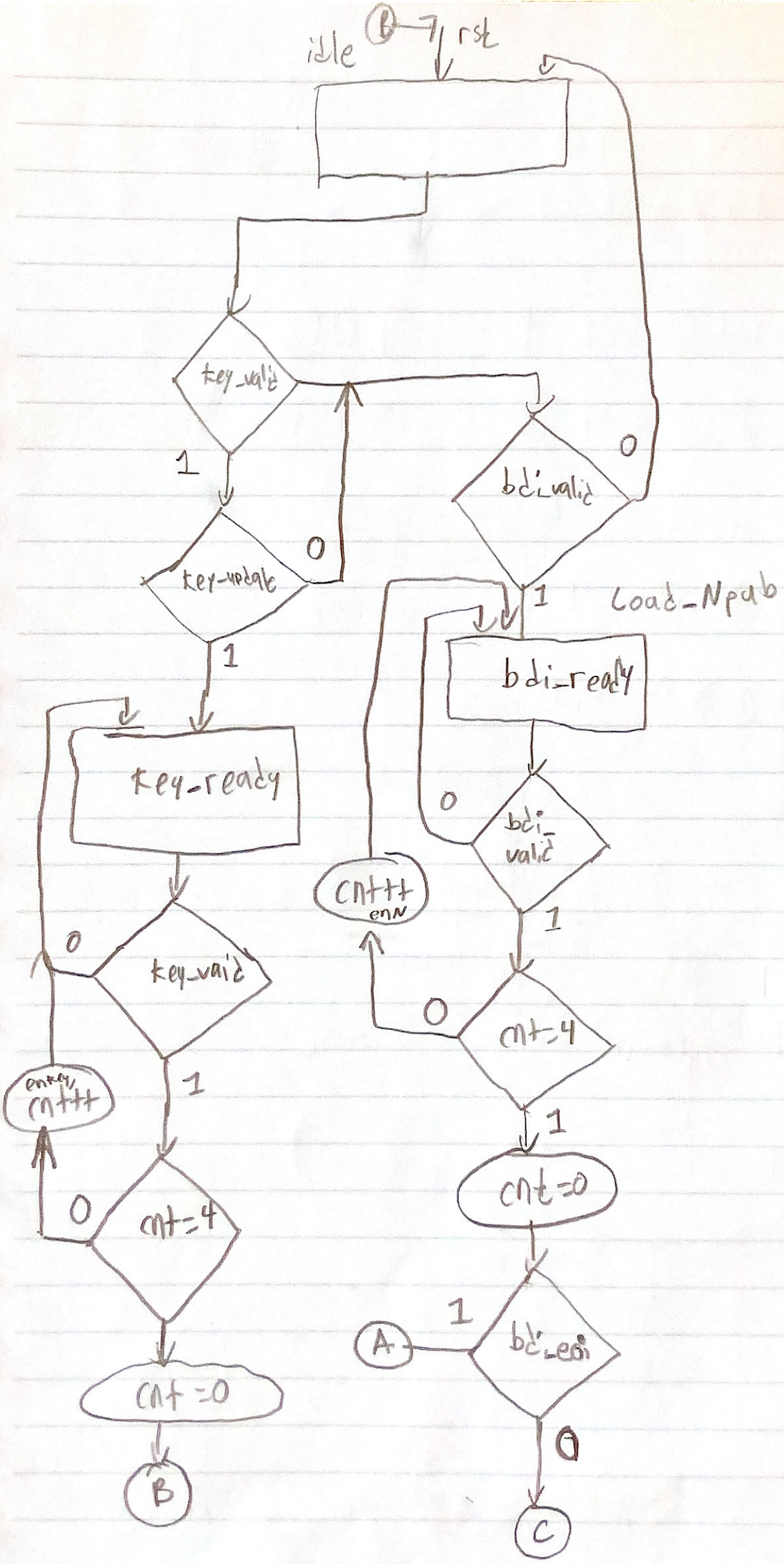
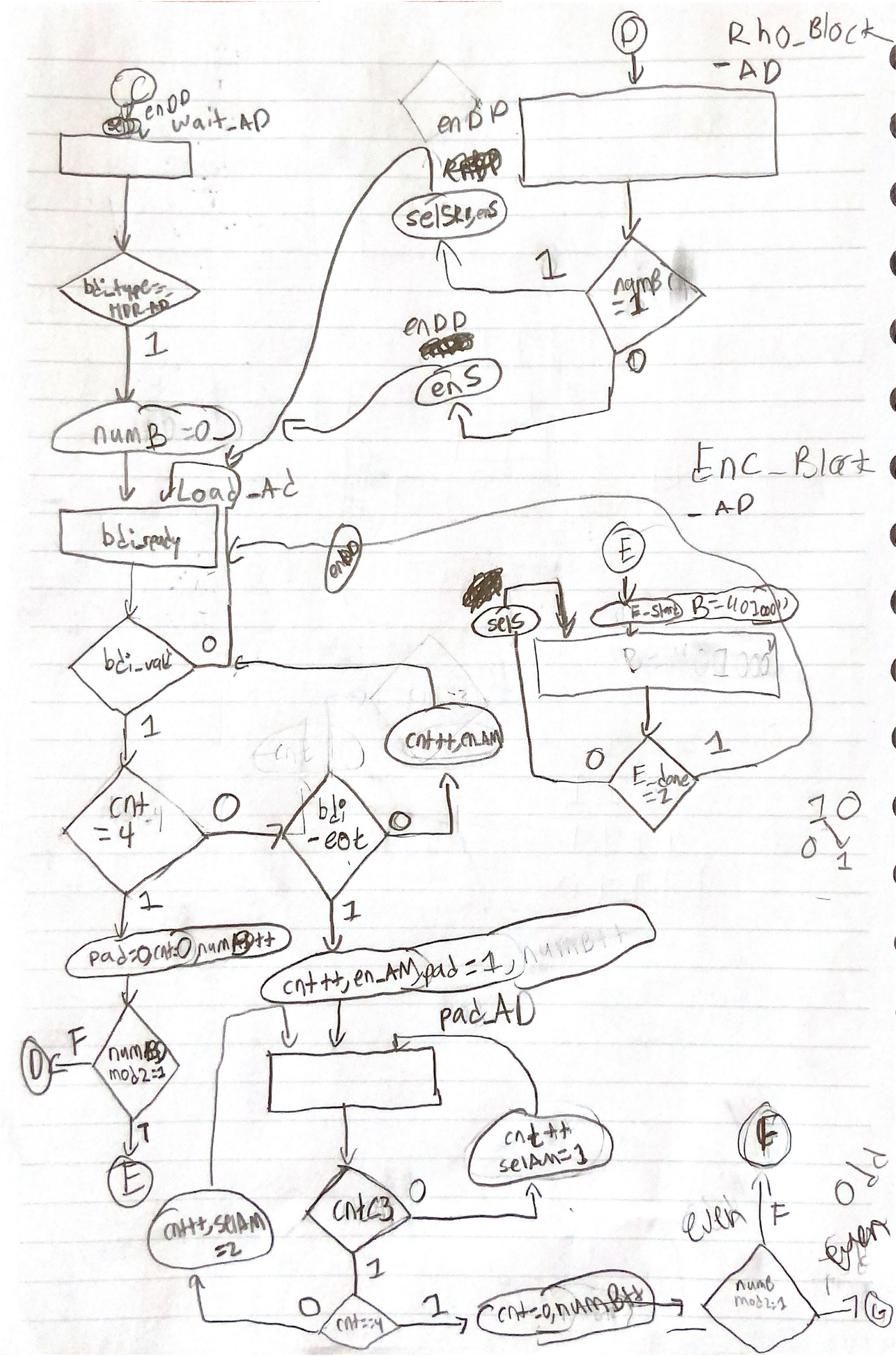
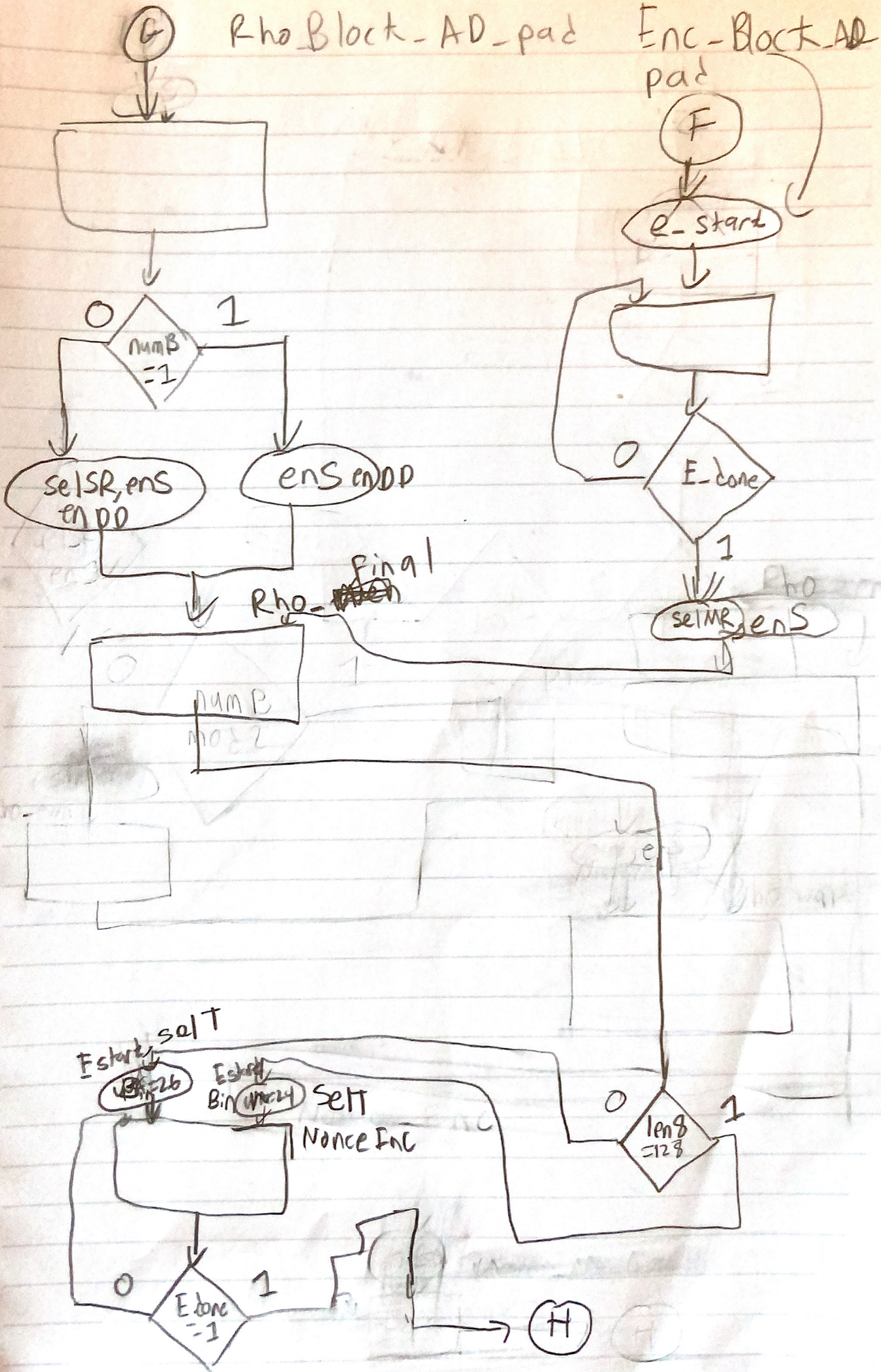
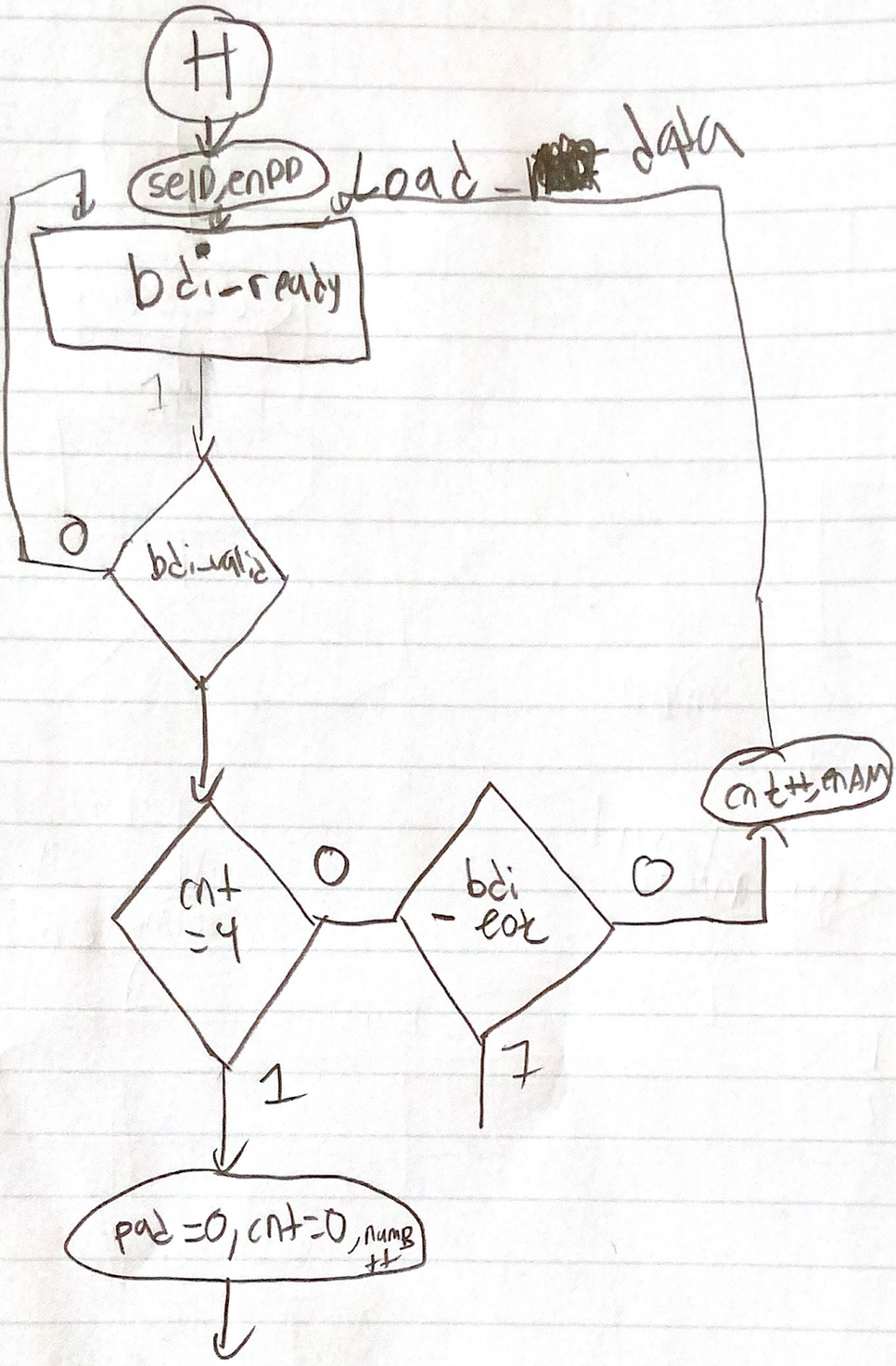

idle
B
rst
key_valid
1
0
key_valid
0
1
key_ready
0
key_valid
1
enkey, cnt++
0
cnt=4
1
cnt=0
B
bdi_valid
0
1
Load_Npab
bdi_ready
0
bdi_valid
1
cnt++ enN
0
cnt=4
1
cnt=0
1
A
bdi_eoi
0
C


C
endD
wait_AD
bdi_type==MDR_AD
1
numB=0
Load_AD
bdi_ready
bdi_valid
0
1
cnt=4
0
bdi_eot
0
1
1
cnt++, en_AM
pad=0 cnt=0 numB++
F
numB mod2=1
T
E
cnt++, selAM=2
cnt<3
0
1
cnt++ selAM=1
cnt==4
0
1
cnt=0, numB++
D
RhO_Block_AD
endD
selS, enS
1
numB=1
0
endD
enS
EnC_Block_AD
endD
E
selS
E_start B=40100(h)
B=40100
0
E_done=2
1
1 0
0 1
cnt++, en_AM pad=1, numB++
pad_AD
F
even
F
0
odd
numB mod2=1
1
G


G
Rho_Block_AD_pad
Enc_Block_AD_pad
F
e_start
0
1
numB =1
selSR, enS enDD
enS enDD
E_done
Final
Rho_
selMR
enS
numB
Fstart
salT
Bin
selT
NonceInc
len8 =128
E done =1
H


H
sel0,enpp
load_
data
bdi-ready
1
0
bdi_valid
cnt
=4
0
bdi
-eot
0
cnt++,enAM
1
7
pad=0, cnt=0, numB++