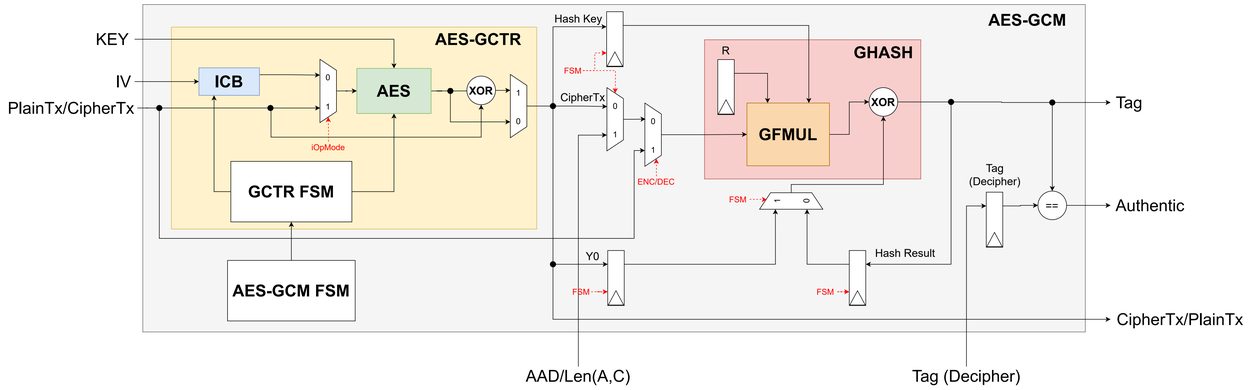
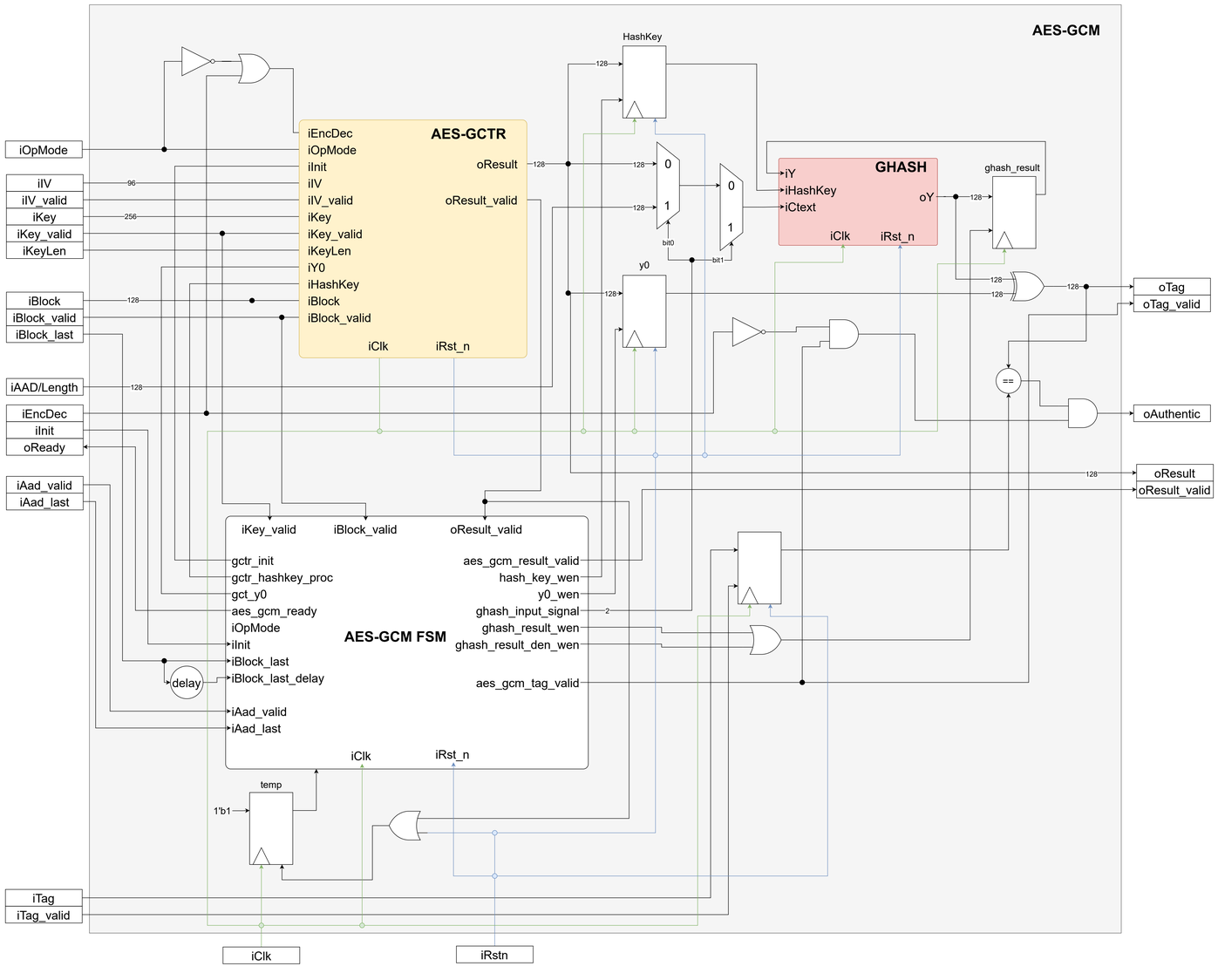
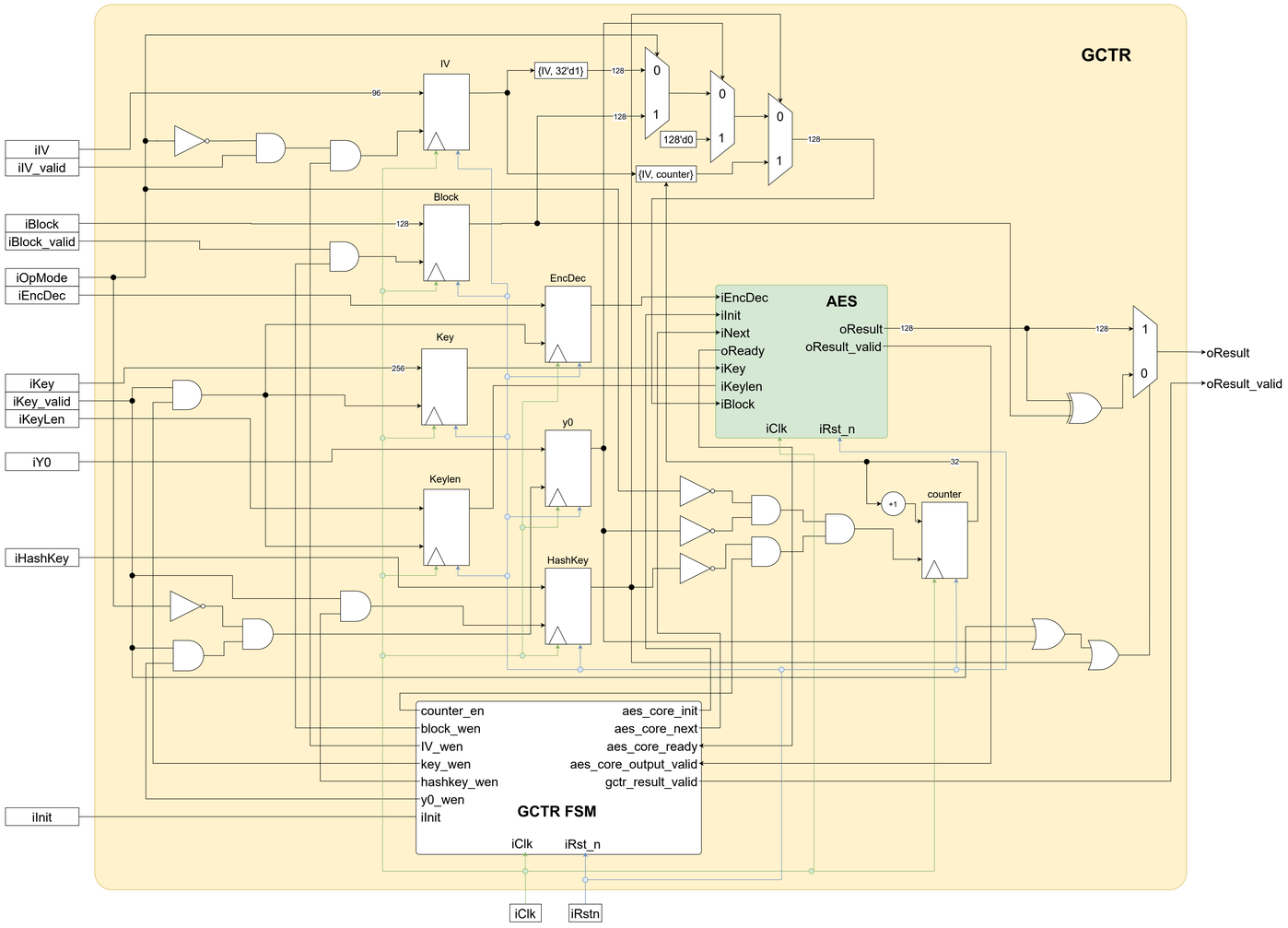
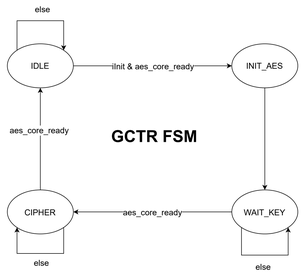

AES-GCM
AES-GCTR
KEY
IV
PlainTx/CipherTx
ICB
AES
XOR
iOpMode
GCTR FSM
AES-GCM FSM
Hash Key
FSM
CipherTx
ENC/DEC
R
GHASH
GFMUL
XOR
Tag
Tag (Decipher)
Authentic
==
Y0
Hash Result
CipherTx/PlainTx
AAD/Len(A,C)
Tag (Decipher)


AES-GCM
HashKey
AES-GCTR
iEncDec
iOpMode
iInit
iIV
iIV_valid
iKey
iKey_valid
iKeyLen
iY0
iHashKey
iBlock
iBlock_valid
oResult
oResult_valid
iClk
iRst_n
GHASH
iY
iHashKey
iCtext
oY
iClk
iRst_n
ghash_result
y0
bit0
bit1
oTag
oTag_valid
oAuthentic
oResult
oResult_valid
AES-GCM FSM
iKey_valid
iBlock_valid
oResult_valid
gctr_init
gctr_hashkey_proc
gct_y0
aes_gcm_ready
iOpMode
iInit
iBlock_last
iBlock_last_delay
iAad_valid
iAad_last
aes_gcm_result_valid
hash_key_wen
y0_wen
ghash_input_signal
ghash_result_wen
ghash_result_den_wen
aes_gcm_tag_valid
delay
temp
1'b1
iTag
iTag_valid
iClk
iRstn




# GCTR FSM

1. IDLE

- counter_wen = 1'b0
- block_wen = 1'b0
- IV_wen = 1'b0
- key_wen = 1'b0
- hashkey_wen = 1'b0
- aes_core_init = 1'b0
- aes_core_next = 1'b0
- gctr_result_valid = aes_core_output_valid

2. INIT_AES

- block_wen = 1'b1
- IV_wen = 1'b1
- key_wen = 1'b1
- hashkey_wen = 1'b1
- aes_core_init = 1'b1
- gctr_result_valid = 1'b0

3. WAIT_KEY

- block_wen = 1'b0
- IV_wen = 1'b0
- key_wen = 1'b0
- hashkey_wen = 1'b0
- aes_core_init = 1'b0

4. CIPHER

- counter_en = 1'b1
- aes_core_next = 1'b1

# AES-GCM FSM

1. IDLE:

- ----------ghash----------
- ghash_result_wen = 1'b0
- ghash_result_dec_wen = 1'b0
- temp_wen = 1'b0
- hash_key_wen = 1'b0
- ghash_input_signal[0] = 1'b0
- ghash_input_signal[1] = 1'b0
- ----------gctr----------
- gctr_init = 1'b0
- gctr_hashkey_proc = 1'b0
- gctr_y0 = 1'b0
- y0_wen = 1'b0
- ----------aes_gcm----------
- aes_gcm_ready = 1'b1
- aes_gcm_tag_valid = 1'b0
- aes_gcm_result_valid = 1'b0

2. HASHKEY

- ----------ghash----------
- (oResult_valid) ? hash_key_wen = 1'b1 : hash_key_wen = 1'b0
- ----------gctr----------
- (oResult_valid) ? gctr_init = 1'b0 : gctr_init = 1'b1
- gctr_hashkey_proc = 1'b1

3. AAD

- ----------ghash----------
- ghash_input_signal[0] = 1'b1
- (iAad_valid)? ghash_result_wen = 1'b1 : ghash_result_wen = 1'b0
- hash_key_wen = 1'b0
- ----------gctr----------
- gctr_init = 1'b0
- gctr_hashkey_proc = 1'b0
- ----------aes_gcm----------
- aes_gcm_ready = 1'b1

4. CIPHER

- ----------ghash----------
- ghash_input_signal[0] = 1'b0
- (iEncDec)? ghash_input_signal[1] = 1'b0 : ghash_input_signal[1] = 1'b1
- temp_wen =1'b1
- (iEncDec & oResult_valid) ghash_result_wen = 1'b1 : ghash_result_wen = 1'b0
- (~iEncDec) ghash_result_dec_wen = ~temp & ~ghash_result_wen : ghash_result_dec_wen = 1'b0
- ----------gctr----------
- (gctr_result_valid & iBlock_last_delay | ~iBlock_valid) gctr_init = 1'b0 : gctr_init = 1'b1
- ----------aes_gcm----------
- (gctr_result_valid) aes_gcm_ready = 1'b1 : aes_gcm_ready = 1'b0
- aes_gcm_result_valid = oResult_valid

5. TAG1

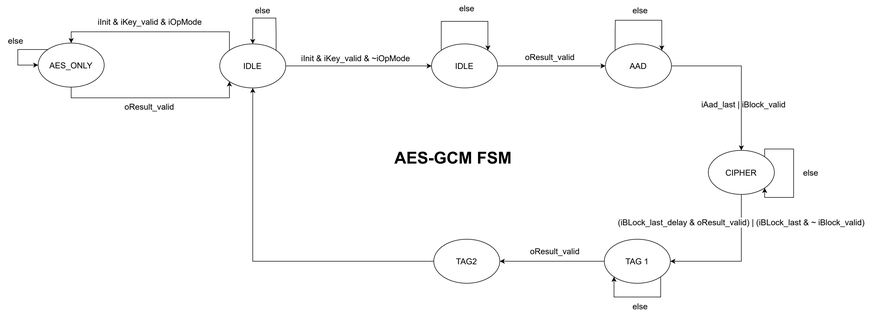
- ----------ghash----------
- ghash_input_signal[0] = 1'b0
- ghash_input_signal[1] = 1'b0
- ghash_result_wen = 1'b0
- ----------gctr----------
- (oResult_valid) ? gctr_init = 1'b0 : gctr_init = 1'b1
- gctr_y0 = 1'b1
- (oResult_valid) ? y0_wen = 1'b1 : y0_wen = 1'b0
- ----------aes_gcm----------
- aes_gcm_ready = 1'b0
- aes_gcm_result_valid = 1'b0

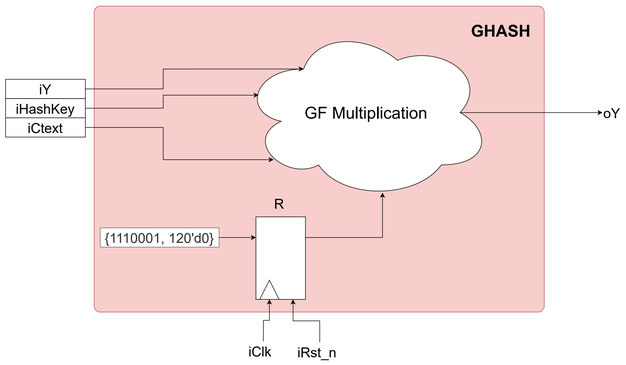
6. TAG2

- ----------ghash----------
- ghash_input_signal[0] = 1'b1
- ghash_result_wen = 1'b1
- ----------gctr----------
- gctr_init = 1'b0
- gctr_y0 = 1'b0
- y0_wen = 1'b0
- ----------aes_gcm----------
- aes_gcm_tag_valid = 1'b1

7. AES_ONLY:

- ----------gctr----------
- gctr_init = 1'b1
- ----------aes_gcm----------
- (oResult_valid) aes_gcm_ready = 1'b1 : aes_gcm_ready = 1'b0
- (oResult_valid) aes_gcm_result_valid = 1'b1 : aes_gcm_result_valid = 1'b0




GHASH
iY
iHashKey
iCtext
GF Multiplication
oY
R
{1110001, 120'd0}
iClk
iRst_n