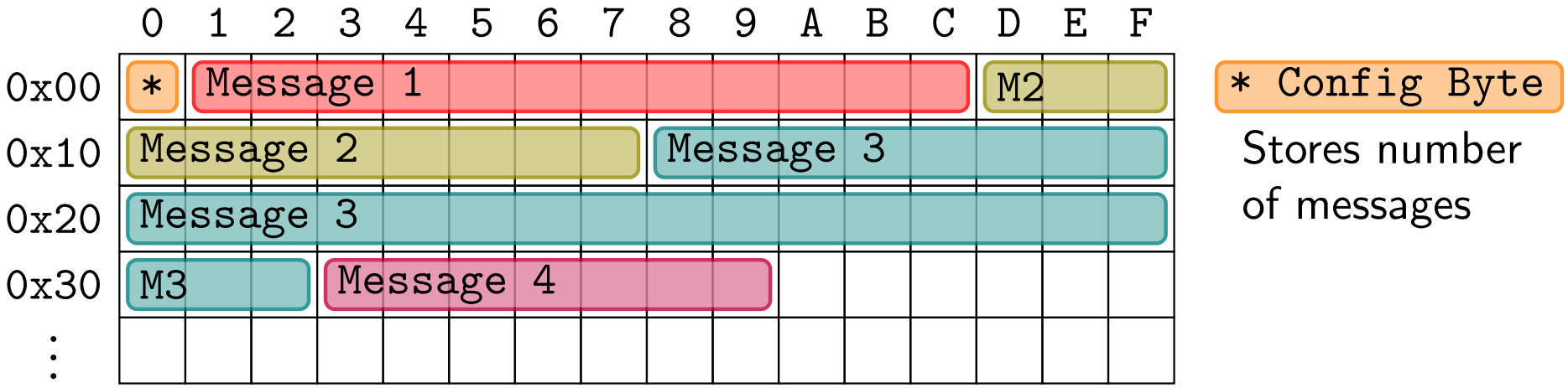
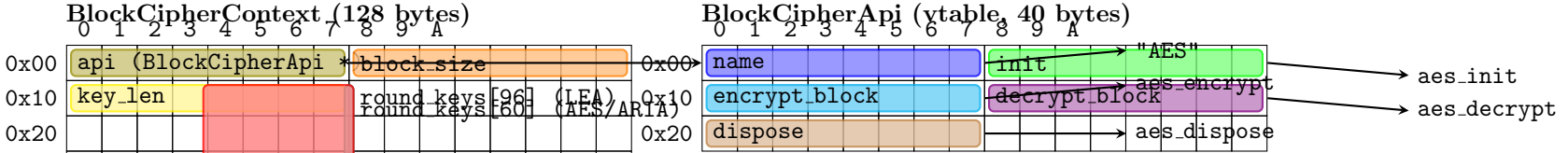

0 1 2 3 4 5 6 7 8 9 A B C D E F
0x00
0x10
0x20
0x30
*
Message 1
M2
Message 2
Message 3
Message 3
M3
Message 4
* Config Byte
Stores number of messages


BlockCipherContext (128 bytes)
0 1 2 3 4 5 6 7 8 9 A
0x00
0x10
0x20
0x30
0x40
0x50
0x60
0x70
api (BlockCipherApi *)
block_size
key_len
round_keys[96] (LEA)
round_keys[60] (AES/ARIA)
nr (AES/ARIA)
nr (LEA)
padding (LEA)
BlockCipherApi (vtable, 40 bytes)
0 1 2 3 4 5 6 7 8 9 A
0x00
0x10
0x20
name
init
"AES"
encrypt_block
decrypt_block
dispose
aes_init
aes_encrypt
aes_decrypt
aes_dispose