Decryption is started by triggering the START task with the MODE register set to `FastDecryption`.

CCM will write the l(m) value of the decrypted packet to the location provided in OUT.PTR, and then store the decrypted packet into memory at the locations given by the OUT.PTR list as illustrated in the following figure.

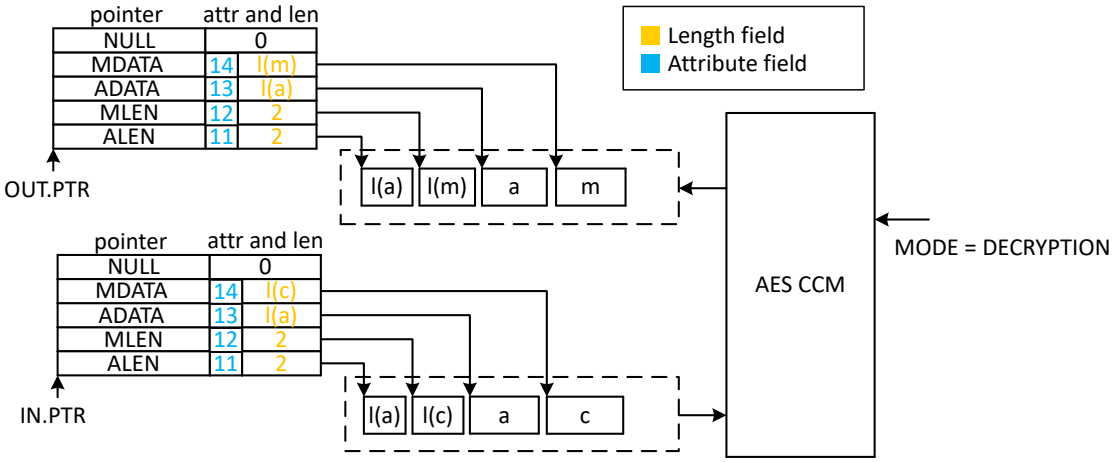

Figure 46: Decryption

For Bluetooth (MODE.PROTOCOL=`Ble`), CCM is only able to authenticate messages where l(c) is at least MACLEN+1 bytes long. If l(c) is less than MACLEN+1, CCM will generate an END event and clear the MACSTATUS (indicating MAC check failure). Furthermore, empty packets (l(c)=0) will be moved unmodified through the AES CCM peripheral even though ERROR event shall be generated. In any other case that leads to a failed MACSTATUS or an ERROR event, the contents of the job addresses given in OUT.PTR are undefined.

For IEEE 802.15.4 (MODE.PROTOCOL=`Ieee802154`), CCM will also perform authentication on messages where only ADATA is present (i.e. l(m)=0 and l(a)>0). In this case MACSTATUS reflects the result of the authentication. If l(c)<MACLEN, then the ERROR event is generated, and the contents of the locations given in OUT.PTR are undefined.

If the following occurs, the ERROR event is generated, and CCM is stopped.

- The IN.PTR job list ends before reading out the complete CCM data structure
- The OUT.PTR job list ends before writing out the complete decrypted CCM data structure
- The EasyDMA engine encounters an error, see EasyDMA and ERROR event on page 239

If the IN.PTR or OUT.PTR job lists do not end before the complete encrypted/decrypted CCM data structures are read, the END event is generated and CCM operation is stopped.

8.4.3 Encrypting packets in radio transmit mode

When the AES CCM is encrypting a packet at the same time as the radio is transmitting it, the radio must read the encrypted packet from the same memory location as the AES CCM is writing to.

The OUT.PTR pointer in the AES CCM must therefore point to the same memory location as the PACKETPTR pointer in the radio, see Example configuration of encryption during radio transmission on page 237.