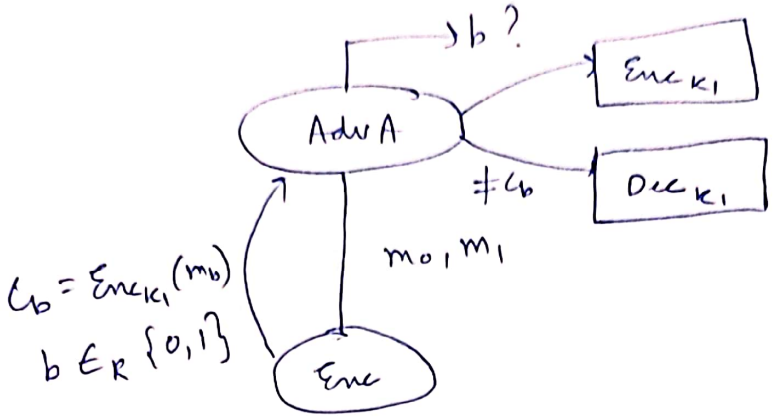
CCA-Secure Scheme



For a CCA-secure scheme, we first encrypt the message with the CPA-secure encryption scheme developed earlier. Then, the ciphertext obtained is passed through MAC (here, CBC-MAC)

$$m, \langle r, F_{K_1}(r) \oplus m \rangle, \langle\langle r, F_{K_1}(r) \oplus m \rangle, t \rangle$$

Encryption

$t = MAC_{K_2}$ or $CBC\text{-}MAC_{K_{21}, K_{22}}$

Adversary A receives no output for ciphertext of messages other than m_b; $b \in_R \{0,1\}$ received from the channel as it cannot obtain their correct tags. Adversary cannot query c_b and hence, A is blocked from receiving any ~~CPA~~ chosen ciphertext decryption to perform attacks.

The encryption scheme is CPA secure and hence CPA isn't possible.

Overall, the scheme is CCA-secure.