CCA.

To prove: for given messages m_0 and m_1, and some encryption c of one of the random messages, guessing the individual message should not be possible.

$$\text{i.e.} \quad P\left[A(c) == b \mid \underbrace{c \notin Q} \right] \leq negl(n)$$

Q be the set of queries made by the adversary A so far.

Proof:

Assuming, MAC is secured & enc scheme is CPA-secure,

∵ our construction returns decryption if the decrypted message & the tag are valid message tag pair.

∵ MAC is secure,

$$\Rightarrow \quad Pr(\cdot\, Vrfy \langle m, t \rangle) = 1 \mid m \notin Q) \leq negl(n)$$

& ∵ since, this hides the ciphertext,

$$P[\text{valid query}] = negl(n).$$

∵ since our encryption is CPA secure,

∴ any CPA attack shouldn't work on this.

$$\therefore \quad P[\, A(c) == b \mid c \notin Q] \leq negl(n)$$

Hence proved.