Use the aforementioned CPA security and secure MAC to design a provably CCA-secure encryption scheme

To build a provably secure CCA-secure private-key encryption scheme(Gen', Enc', Dec'), the following instructions will be helpful.
Let a private-key encryption scheme be (Gen_E, Enc, Dec) and a message authentication code be (Gen_M, Mac, Vrfy)

1. Gen' : on input 1^n, run $Gen_E(1^n)$ and $Gen_M(1^n)$ to obtain keys k_1, k_2, respectively.
2. Enc' : on input a key (k_1,k_2) and a plaintext message m, compute c <- Enc_{k_1} (m) and t <- Mac_{k_2}(c) and output the ciphertext <c,t>
3. Dec' : on input a key (k_1, k_2) and a ciphertext <c,t>, first check whether $Vrfy_{k\_2}$(c,t) = 1. If yes, then output Dec_{k_1}(c).

The encrypt and decrypt functions perform their usual functions in addition to checking if the two keys k1 and k2 are the same or not.

The arguments for generate and verify mode are also handled.

The code has been explained in the comments present in the script wherever necessary.