sEUF-CMA security

1. Collision-resistant chameleon hash functions can be used to transform any EUF-CMA secure signature scheme into one that is sEUF-CMA secure.
   
   ☑️ True
   ✗ False

2. sEUF-CMA security guarantees... (choose as many options as you think apply)
   
   ✗ A ...that only one signature per message exists for any fixed public key.
   ✗ B ...that at most one signature per message can be found efficiently given a fixed keypair (pk,sk).
   ☑️ C ...everything that EUF-CMA security guarantees (and possibly more).
   ☑️ D ...everything the EUF-naCMA security guarantees (and possibly more).

3. How many instances (i.e., keys) of a chameleon hash function does the transformation from the previous question use?
   
   2

4. Would the proof of the "CH + EUF-CMA → sEUF-CMA" theorem also work for a construction that omits the second CHF F (so that h and not \(\tilde{m}\) is signed)? Why/why not?
   
   No, because we cannot use the collision-resistance of a (single) CHF whose trapdoor we have to use during signing.