Fully Homomorphic Encryption – Problem Set

Hybrid Encryption. Consider an FHE scheme HE with keys (pk, sk) and a (very efficient) symmetric encryption scheme SYM. We now consider a new FHE scheme, whose only difference from the original is the encryption algorithm as follows. To encrypt a message m, first generate a fresh key $symsk$ for SYM. Then create $c^* = \mathsf{HE.Enc}_{pk}(symsk)$ and $c = \mathsf{SYM.Enc}_{symsk}(m)$. Output the pair (c^*, c).

1. For a given ciphertext $c = \mathsf{SYM.Enc}_{symsk}(m)$, consider the function $C_c(x) = \mathsf{SYM.Dec}_x(c)$. What is the value of $C_c(symsk)$?
2. What is the output of $\mathsf{Eval}(C_c, c^*)$? Recall that the output of Eval is a ciphertext. What does this ciphertext encode? Under which key?
3. Show that the new scheme is also an FHE.
4. What is the complexity of encryption of the new scheme if the length of the message is much greater than that of the symmetric key, namely when $|m| \gg |symsk|$?

Bootstrapping. Analyze the general technique to bootstrap bounded depth HE.

1. Let D be the decryption circuit of an encryption scheme. Namely, $D(sk, c) = m$. Let d be the depth of this circuit.

   Consider the circuit $C(sk, c_1, c_2)$, defined as

   $$C(sk, c_1, c_2) = \big(D(sk, c_1)\ \mathbf{NAND}\ D(sk, c_2)\big).$$

   What is the depth of the circuit C?
2. Let c_1 be an encryption of a bit m_1 and c_2 be an encryption of a bit m_2. What is the result of $C(sk, c_1, c_2)$?
3. Given some c_1, c_2, we define the circuit $C'_{c_1,c_2}(sk) = C(sk, c_1, c_2)$ (note that in C'_{c_1,c_2}, the values c_1, c_2 are hard-coded and are not a part of the input). What is the output of $C'_{c_1,c_2}(sk)$?
4. If our scheme is homomorphic, and letting $c^* = \mathsf{Enc}_{pk}(sk)$ be *an encryption of the secret key sk*. what is the output of $\mathsf{Eval}(C'_{c_1,c_2}, c^*)$? Recall that the output of homomorphic evaluation is always a ciphertext. What does this ciphertext encode?
5. Show that if the scheme is homomorphic only for depth $d + 1$ circuits, and c^* is given, then any circuit can be evaluated homomorphically. Recall that any circuit can be written using only **NAND** gates.