1 Bad Fujisaki-Okamoto variant

Fujisaki-Okamoto (FO) uses two hash functions $G$ and $H$. You want to implement FO and you notice: Your crypto library provides only a single hash function (e.g., SHA3 with a specific parameter set). So you don’t have two different hash functions available. So, you instead implement the following slightly changed FO:

- **Key generation:** Use $\text{KeyGen}$.
- **Encapsulation:** $\text{Encaps}(pk)$ runs: $m \xleftarrow{\$} \mathcal{M}$. ($\mathcal{M}$ is the message space of $\text{Enc}$.) $c \leftarrow \text{Enc}(pk, m; H(m))$. $k := H(m)$. Return $(c, k)$.
- **Decapsulation:** $\text{Decaps}(sk, c)$ runs: $m \leftarrow \text{Dec}(sk, c)$. If $m = \bot$ or $c \neq \text{Enc}(pk, m; H(m))$, return $\bot$. Otherwise set $k := H(m)$ and return $k$.

Why is this a bad idea? More precisely, show that this is not IND-CCA secure.

Note: For example, you could show how, given $c$ and $k$, you can check whether you indeed got $k$ (and not $c$ and $k'$ for some random $k'$).

2 O2H Theorem

Show that if $f$ is a one-way function and $G$ is a random oracle, then $x \mapsto (f(x), G(x))$ is one-way, too.

Specifically, show the following: For a $q$-query adversary $A$, $\Pr[b = 1 : G_1]$ is negligible where:

- Game $G$: $G \xleftarrow{\$} (\{0, 1\}^n \rightarrow \{0, 1\}^n)$. $x \xleftarrow{\$} \{0, 1\}^n$. $x' \leftarrow A^G(f(x), G(x))$. win iff $x' = x$.

**Hint:** Use the O2H theorem. The sequence of games involved is the same as in the proof in the lecture. (The games themselves are, of course, somewhat different since we have a different starting point. But the ideas behind the games are not much different here.)
Show that the random oracle is a pseudorandom generator.

Specifically, show the following: For a $q$-query adversary $A$, $|\Pr[b = 1 : G_1] - \Pr[b = 1 : G_2]| \leq O(q\sqrt{2^{-n}})$ where:

- Game $G_1$: $G \leftarrow (\{0,1\}^n \rightarrow \{0,1\}^{2n})$. $x \leftarrow \{0,1\}^n$. $b \leftarrow A^{G}(G(x))$.
- Game $G_2$: $G \leftarrow (\{0,1\}^n \rightarrow \{0,1\}^{2n})$. $y \leftarrow \{0,1\}^{2n}$. $b \leftarrow A^{G}(y)$.

**Hint:** Use the O2H theorem. You can do a preparation for applying the O2H Theorem that is quite similar to what’s happening in the lecture, but the resulting sequence of games is a little different because we are not trying to show that a winning probability is small, but that a difference in probabilities is small. So pay attention: In the guessing game, you will need to show that some probability is small, but for the other games you will only need to show that probabilities are similar.