Question 4

(1)

We denote the augmented signature scheme's parameters and functions with a star to differentiate them from the parameters and routines of the input signature scheme.

For key generation, set $\mathrm{sk}^* = (\mathrm{pk}, \mathrm{sk})$ and $\mathrm{pk}^* = H(\mathrm{pk})$, where $\mathrm{pk}, \mathrm{sk} \leftarrow \mathrm{KeyGen}$ is generated from the input signature scheme, and H is the input collision-resistant hash function.

For $\mathrm{Sign}^*(\mathrm{sk}^*, m)$, first compute $\sigma = \mathrm{Sign}(\mathrm{sk}, m)$ using the input signature scheme's signing routine, then output $\sigma^* = (\mathrm{pk}, \sigma)$ as the signature.

For $\mathrm{Verify}^*(\mathrm{pk}^*, \sigma^*, m)$, first unpack the signature $(\hat{\mathrm{pk}}, \hat{\sigma}) = \sigma^*$ and check that $H(\hat{\mathrm{pk}})$ is equal to pk^*. Then, run the input signature scheme's verification routine $\mathrm{Verify}(\hat{\mathrm{pk}}, \hat{\sigma}, m)$. The verification passes if and only if both checks pass.

(2)

We show that the modified signature scheme is EUF-CMA by showing that if there exists an EF-CMA adversary for the modified scheme $\mathcal{A}^*_{\text{EF-CMA}}$, then we can build an EF-CMA adversary for the original scheme $\mathcal{A}_{\text{EF-CMA}}$ with equal advantage.

In the EF-CMA game of the input scheme, key generation outputs the keypair $(\mathrm{pk}, \mathrm{sk})$. $\mathcal{A}_{\text{EF-CMA}}$ computes $\mathrm{pk}^* = H(\mathrm{pk})$ and passes pk^* to $\mathcal{A}^*_{\text{EF-CMA}}$.

When $\mathcal{A}^*_{\text{EF-CMA}}$ queries the signature of some message m_i, $\mathcal{A}_{\text{EF-CMA}}$ queries the signature σ_i of m_i from the signing oracle for the input signature scheme. $\mathcal{A}_{\text{EF-CMA}}$ then gives $\sigma_i^* = (\mathrm{pk}, \sigma_i)$ back to $\mathcal{A}^*_{\text{EF-CMA}}$ as the answer to the query.

When $\mathcal{A}^*_{\text{EF-CMA}}$ outputs the forgery $\hat{\sigma^*} = (\hat{\mathrm{pk}}, \hat{\sigma}, \hat{m})$, we claim that $\hat{\mathrm{pk}} = \mathrm{pk}$, because otherwise we will have found collision $\hat{\mathrm{pk}} \neq \mathrm{pk}$ such that $H(\hat{\mathrm{pk}}) = H(\mathrm{pk})$. Thus $\mathcal{A}^*_{\text{EF-CMA}}$ is valid if and only if $\hat{\sigma}, \hat{m}$ pass the verification of the original signature scheme. Therefore, $\mathcal{A}_{\text{EF-CMA}}$ has the same advantage as $\mathcal{A}^*_{\text{EF-CMA}}$.