COSC 530: Homework 3

Problem 1. (100 points.)

(60 points.) Let \( H : \mathcal{K} \times \{0,1\}^* \to \{0,1\}^n \) be a collision-resistant hash function. Use \( H \) to construct a hash function \( H' \) that is also collision-resistant, but if one truncates the output of \( H' \) by one bit then \( H' \) is no longer collision-resistant. That is, prove that \( H' \) is collision resistant, but \( H''(x) := H'(x)[0\ldots n-2] \) is not by giving an explicit attack. (40 points.) What does this tell you about practical cryptographic hash functions such as SHA256?

Problem 1. (100 points.)

The MD transform gives a sequential method for extending the domain of a collision-resistant hash function. Design an alternative, tree-based method that is parallelizable. State and prove an analogous theorem regarding its collision-resistance.

Problem 3. (100 points.) Define \( \mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D}) \) where \( \mathcal{K} \) returns a random 128-bit key \( K \) and

\[
\begin{align*}
\text{Algorithm } \mathcal{E}_K(M) : \\
&\text{If } |M| \neq 512 \text{ then return } \perp \\
&M[1]\|M[2]\|M[3]\|M[4] \leftarrow M \\
&C_e[0] \leftarrow \{0,1\}^{128} ; C_m[0] \leftarrow 0^{128} \\
&\text{For } i = 1, 2, 3, 4 \text{ do:} \\
&\quad C_e[i] \leftarrow \text{AES}_K(C_e[0] + i) \oplus M[i] \\
&\quad C_m[i] \leftarrow \text{AES}_K(C_m[i - 1] \oplus M[i]) \\
&\quad C_e \leftarrow C_e[0]\|C_e[1]\|C_e[2]\|C_e[3]\|C_e[4] \\
&T \leftarrow C_m[4] ; \text{ Return } (C_e, T)
\end{align*}
\]

Above, “\( C_e[0] + i \)” denotes interpreting \( C_e[0] \) as an integer modulo \( 2^{128} \), adding \( i \) modulo \( 2^{128} \), and interpreting the result as a 128-bit string.

\[
\begin{align*}
\text{Algorithm } \mathcal{D}_K((C_e, T)) : \\
&\text{If } |C_e| \neq 640 \text{ then return } \perp \\
&C_m[0] \leftarrow 0^{128} \\
&\text{For } i = 1, 2, 3, 4 \text{ do:} \\
&\quad M[i] \leftarrow \text{AES}_K(C_e[0] + i) \oplus C_e[i] \\
&\quad C_m[i] \leftarrow \text{AES}_K(C_m[i - 1] \oplus M[i]) \\
&\text{Else return } \perp 
\end{align*}
\]

(Part A - 40 points.) Is \( \mathcal{SE} \) IND-CPA secure?

(Part B - 40 points.) Is \( \mathcal{SE} \) INT-CTXT secure?

(Part C - 20 points.) Is \( \mathcal{SE} \) an Encrypt-and-MAC construction?

For Parts A and B above, if your answer is “yes” then you should give some convincing intuition (a proof is best). You can make the usual assumptions about the security of AES. If your answer is “no” then you should give an explicit attack.