Criptografía y Seguridad Computacional - IIC3253
Tarea 1
Solución pregunta 4

Considere el juego *Hash-Col*(n) mostrado en clases para definir la noción resistencia a colisiones. Utilizando este tipo de juegos, defina la noción de resistencia a preimagen para una función de hash (Gen, h). Además, demuestre que si (Gen, h) es resistente a colisiones, entonces (Gen, h) es resistente a preimagen.

Solución. Considere una función de hash (Gen, h) tal que si $Gen(1^n) = s$, entonces $h^s : \{0,1\}^* \to \{0,1\}^{\ell(n)}$ donde $\ell(n)$ es un polinomio fijo. Además, suponga que h se puede calcular en tiempo polinomial en el largo de la entrada, vale decir, $h(m)$ se puede calcular en tiempo $O(|m|^c)$ para alguna constante fija c. Definimos un juego *Hash-Pre-Img*(n) dado por los siguientes pasos:

1. El verificador genera $s = Gen(1^n)$ y un hash $x \in \{0,1\}^{\ell(n)}$
2. El adversario elige $m \in \{0,1\}^*$ o $m = \perp$
3. El adversario gana el juego si alguna de las siguientes condiciones se cumple:
    - $m \in \{0,1\}^*$ y $h^s(m) = x$
    - $m = \perp$ y no existe $m' \in \{0,1\}^*$ tal que $h^s(m') = x$

   En caso contrario, el adversario pierde.

Además, decimos que (Gen, h) es resistente a preimagen si para todo adversario que funciona como un algoritmo aleatorizado de tiempo polinomial, la función Pr(Adversario gane *Hash-Pre-Img*(n)) es despreciable (nótese que esta es una función de n).

Vamos a demostrar que si (Gen, h) es resistente a colisiones, entonces (Gen, h) es resistente a preimagen. De manera más precisa, vamos a hacer esto considerando el contrapositivo, vale decir, vamos a mostrar que si (Gen, h) no es resistente a preimagen, entonces (Gen, h) no es resistente a colisiones.

Suponga que (Gen, h) no es resistente a preimagen. Entonces existe un adversario $\mathcal{A}$ tal que $\mathcal{A}$ es un algoritmo aleatorizado de tiempo polinomial y Pr($\mathcal{A}$ gane *Hash-Pre-Img*(n)) no es una función despreciable. A partir del algoritmo $\mathcal{A}$, vamos a definir un algoritmo aleatorizado $\mathcal{B}$ tal que $\mathcal{B}$ funciona en tiempo polinomial y Pr($\mathcal{B}$ gane *Hash-Col*(n)) no es una función despreciable. Suponga que $\mathcal{A}$ funciona en tiempo $p(n)$, donde $p(n)$ es un polinomio fijo. Dado $s = Gen(1^n)$, el algoritmo $\mathcal{B}$ construye $m' = 0^{p(n)+1}$ (vale decir, m' tiene $p(n) + 1$ símbolos 0), se pone en el papel del verificador en el juego *Hash-Pre-Img*(n) y define $x = h^s(m')$ (nótese que $x \in \{0,1\}^{\ell(n)}$). Una vez que el algoritmo $\mathcal{A}$ responde con un mensaje $m \in \{0,1\}^*$ en el juego *Hash-Pre-Img*(n), el algoritmo $\mathcal{B}$ retorna el par de mensajes m, m'.

Dado que el mensaje m' es de largo $p(n) + 1$, la función de hash h se puede calcular en tiempo polinomial (en el largo de la entrada) y $\mathcal{A}$ es un algoritmo aleatorizado de tiempo polinomial, se tiene que $\mathcal{B}$ es un algoritmo aleatorizado de tiempo polinomial. Para terminar la demostración solo necesitamos mostrar que Pr($\mathcal{B}$ gane *Hash-Col*(n)) no es una función despreciable. Nótese que si $\mathcal{A}$ gana el juego *Hash-Pre-Img*(n), entonces $\mathcal{A}$ genera un mensaje $m \in \{0,1\}^*$ tal que $h(m) = x$ (ya que $x = h(m')$ con $m' \in \{0,1\}^*$). Además, el algoritmo $\mathcal{A}$ ejecuta a lo más $p(n)$ pasos, por lo que

$|m| \leq p(n)$ y se puede concluir que $m \neq m'$ ya que $|m'| = p(n) + 1$. Así, tenemos que si $\mathcal{A}$ retorna un mensaje $m \in \{0,1\}^*$ tal que $h(m) = x$, entonces m, m' es una colisión para la función de hash (Gen, h) y $\mathcal{B}$ gana el juego *Hash-Col*(n). En términos de probabilidades, lo que concluimos es que:

$$\Pr(\mathcal{B} \text{ gane } \mathit{Hash\text{-}Col}(n)) \quad = \quad \Pr(\mathcal{A} \text{ gane } \mathit{Hash\text{-}Pre\text{-}Img}(n)).$$

De esta forma, se deduce que $\Pr(\mathcal{B} \text{ gane } \mathit{Hash\text{-}Col}(n))$ es una función no despreciable, puesto que $\Pr(\mathcal{A} \text{ gane } \mathit{Hash\text{-}Pre\text{-}Img}(n))$ es una función no despreciable. Esto concluye la demostración de la propiedad.