Pontificia Universidad Católica de Chile
Departamento de Ciencia de la Computación
IIC3253 - Criptografía y Seguridad Computacional

Samuel Zúñiga [sezuniga1@uc.cl] 16637747

Tarea 1 - Pregunta 4

Noción de resistencia a pre-imagen:

Considere una función de hash (Gen, h). Definimos el juego $Hash - Preimg(n)$:

1. El verificador genera $s = Gen(1^s)$ y un $x \in \mathcal{X}$ y se lo entrega al adversario.
2. El adversario elige un $m \in \mathcal{M}$.
3. El adversario gana si $h^s(x) = m$, en caso contrario pierde.

Una función de hash (Gen, h) se dice resistente a pre-imagen si para todo adversario que funciona como un algoritmo aleatorizado de tiempo polinomial, no existe un algoritmo eficiente que dado $x \in \mathcal{X}$ encuentra $m \in \mathcal{M}$ tal que $h(m) = x$. Formalizando, la definición puede escribirse como:

Una función de hash (Gen, h) se dice resistente a pre-imagen si para todo adversario que funciona como un algoritmo aleatorizado de tiempo polinomial, existe una función despreciable $f(n)$ tal que:

$$P(\text{Adversario gane Hash-Preimg(n)}) \leq f(n)$$

Demostración

PD: Si (Gen, h) es resistente a colisiones, entonces (Gen, h) es resistente a preimagen.

Para esta demostración definiremos lo siguiente:

- Resistencia a colisiones: Una función de hash (Gen, h) es resistente a colisiones si es difícil para un adversario encontrar m_1 y m_2 tales que $h^s(m_1) = h^s(m_2)$.
- Resistencia a segunda preimagen: Una función hash es resistente a la segunda preimagen si, dado m_1, es difícil para un adversario encontrar m_2 tal que $h^s(m_1) = h^s(m_2)$.
- Resistencia a preimagen: Una función hash es resistente a preimagen si, dados s y $h^s(m_1)$, con m_1 desconocido, es difícil para un adversario encontrar m_2 tal que $h^s(m_1) = h^s(m_2)$.

Primero demostraremos que si (Gen, h) es resistente a colisiones, entonces (Gen, h) es resistente a segunda preimagen, y luego si se cumple resistencia a segunda preimagen, entonces se cumple resistencia a preimagen.

- **PD: h^s es resistente a colisiones $\implies$ h^s es resistente a segunda preimagen.**

  Para demostrar esto lo haremos por el contraposición: por lo que debemos demostrar que:

  $$\text{Si } h^s \text{ no es resistente a segunda preimagen} \implies h^s \text{ no es resistente a colisiones.}$$

  Como h^s no es resistente a segunda preimagen, entonces podemos tomar algún $m_1 \in \mathcal{M}$ y eventualmente podremos encontrar un m_2 distinto a m_1, tal que $h^s(m_1) = h(m_2)$. Lo anterior nos dice que h^s no es resistente a colisiones. De esta forma demostramos que si h^s es resistente a colisiones $\implies$ h^s es resistente a segunda preimagen. Con lo anterior continuamos con:

- **PD: h^s es resistente a segunda preimagen $\implies$ h^s es resistente a preimagen.**

  Supongamos que tenemos h^s con resistencia a segunda preimagen pero sin resistencia a preimagen (puedo encontrar otro mensaje que tenga el mismo hash que mi mensaje original). Con esto, dado un m_1 puedo calcular $h^s(m_1)$, y debido a la no resistencia a preimagen puedo encontrar m_2 tal que $h^s(m_1) = h(m_2)$.

  Esto es casi una segunda preimagen, lo único que debemos tener en cuenta es si $m_1 \neq m_2$. Vemos que h^s tiene infinitas entradas y un número finito de salidas, por lo que la probabilidad de que $m_2 \neq m_2$ es alta. Este es el caso en las funciones reales de hash, por lo que resistencia a segunda preimagen debe implicar resistencia a preimagen.

Como resistencia a colisiones implica resistencia a segunda preimagen, y resistencia a segunda preimagen implica a resistencia a preimagen, entonces resistencia a colisiones implica resistencia a preimagen.

Fuentes

Modern Cryptography by Katz & Lindell, sección 4.6.2, página 124.