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

Pregunta 4

26 de abril de 2022

Pablo Brancoli - 18642578

Definamos el juego Hash-PreIm(n):

1. El verificador genera $s = Gen(1^n)$ y $c = h^s(m1)$ con un m1 cualquiera, y le pasa s, c al adversario
2. El adversario elige un m2 cualquiera
3. El adversario gana el juego si $h^s(m2) = c$

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

$$Pr(AdversarioGaneHashPreIm(n)) \leq f(n)$$

Es decir no existe un algoritmo que con fuerza bruta pueda encontrar un m2 tal que $h^s(m2) = c$, de manera eficiente.

Ahora buscamos demostrar que si (Gen, h) es resistente a colisiones, también es resistente a preimagen:

Para esto podemos ocupar la misma noción de juego de Hash-Col(n), solo que la cambiamos un poco:

1. El verificador genera $s = Gen(1^n)$ y un mensaje m1, y se los entrega al adversario
2. El adversario elige un m2 cualquiera, con $m1 \neq m2$
3. El adversario gana el juego si $h^s(m2) = h^s(m1)$

Sabemos por la definición de Hash-Col(n) que el adversario no puede encontrar $h^s(m2) = h^s(m1)$ de manera eficiente, por lo que si buscamos que m2 sea la pre imagen de $h^s(m1)$ nos va a ser imposible hacerlo de manera eficiente.