Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencia de la Computación
Marcelo Arenas — Martin Ugarte

IIC3253 — Criptografía y Seguridad Computacional — Diego Iruretagoyena

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.

La criptografía moderna involucra el estudio de técnicas matemáticas para asegurar información digital, sistemas y procesos distribuidos en contra de ataques adversarios. Primero, contextualicemos la técnica aprendida en clase para modelar un juego. Queremos formalizar la idea de seguridad y lograr estructurar la idea de un adversario que podría ganar información acerca de la forma en la que se eligen las llaves. Se representa un escenario enmarcado en un juego de turnos que representa nociones de seguridad frente a ataques basados en ganancia de información de parte de un adversario con capacidad computacional infinita. Además, suponemos principios de Kerchoff, en donde todo menos la llave es públicamente conocido.

Definimos **función de hash** es un **par (Gen, h)**, Gen función que nos permite generar llaves según algún parámetro de seguridad denotado por 1^n. Gen se puede calcular en polinomial en el largo del input, h también. El parametro es unario y puede representar, por ejemplo, el largo del hash que usaremos i.e. 128 bits. Con esto podemos asegurar seguridad ya que algunos algoritmos son dependientes del largo. Si $m \in \{0,1\}^{l'(n)}$ para polinomio fijo l' tal que $l'(n) \leq l(n)$, entonces Gen, h función de hash largo fijo. En este caso, son polinomiales.

Función despreciable significa que ($\forall$ polinomio p)($n0$) i.e. su valor es menor a $\frac{1}{\text{polinomio}}$. i.e. $\frac{1}{2^n}$

Juego Hash-Col(N) mostrado en clases para definir la noción de resistencia a colisiones consistía de considerar una función de hash (Gen, h) y definimos:

- Verificador genera $s = Gen(1^n)$ y se lo entrega al adversario
- Adversario elige mensajes m_1 y m_2 con $m_1 \neq m_2$
- Adversario gana el juego si $h^s(m_1) = h^s(m_2)$, y en caso contrario, pierde.

Definimos además,

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

$$\Pr(\text{Adversario gane Hash-Col(n)} \leq f(n))$$

Resistencia a Preimagen

Recordamos que una propiedad fundamental de las funciones hash es que debe existir un algoritmo eficiente que, dado $m \in M$, calcula $h(m)$ y no debe existir un algoritmo eficiente que, dado $x \in H$, encuentra m $\in M$ tal que $h(m) = x$. Esta propiedad se denota como ser resistente a preimagen. Es decir, un ataque de preimagen se basa en obtener algún mensaje anterior y poder encontrar la llave actual por medio de algún algoritmo. En contexto de nuestro juego, definimos ser resistente a preimagen como que no existe adversario que con información de nuestros mensajes pasados pueda decifrar nuestra llave de encriptación. Debemos identificar que ser resistente a colisiones es una noción muy fuerte de seguridad. Estamos asegurando que la función es despreciable. Comprobaremos que si ya es resistente a colisiones, ya era resistente a preimagen.

Por contradicción, tenemos una función de hash que es resistente a las colisiones pero no es resistente a preimagen.

Dadas las definiciones que hemos dado, podemos caer en cuenta que ser resistente a colisiones es una noción de seguridad muy fuerte, y tener esa propiedad implica ser resistente a colisiones, dado la capacidad de conocimiento que podemos ganar al ver los cifrados.

La probabilidad de que $h^s(m_i) = h^s(m_j)$ pasará con una probabilidad será $P(h^s(m_i) = h^s(m_j))$.

Ser no resistente a preimagen implica que puedo encontrar un m tal que $h^s(m_i)$ con una probabilidad no despreciable.Como tenemos capacidad de computo infinita, podemos iterar constantemente buscando mensajes que logren eventualmente encontrar un mj tal que $h^s(m_j) = h^s(m_i)$. Pero si puedo encontrar un m tal que $h^s(m_i)$.

Esto es verdad si es que la función f está constantemente disminuyendo. Si es resistente a colisiones, sabemos que es posible ganare Hash Col con probabilidad despreciable, pero ahora si no es resistente a preimagen, sería probabilidad no despreciable, lo que es contraintuitivo. Significa que podemos romper Hash Col. Pero eso va contra nuestro supuesto. Entonces, determinamos que este caso no es posible y resistencia a colisiones implica resistencia preimagen