NOMBRE: Tomás Vergara

Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencia de la Computación

IIC3253 — Criptografía — 1' 2022

Tarea 3 – Respuesta Pregunta 4

Una noción que podemos definir para formalizar la resistencia a preimagen es el juego $HashPreImg(n)$ definido a continuación:

1. El verificador genera $s = Gen(1^n)$ y se lo pasa al adversario.

2. El verificador genera aleatoriamente un valor $x \in \mathcal{H}$, de tamaño n.

3. El adversario elige un mensaje m.

4. El adversario gana si es que $h^s(m) = x$

Con este juego, se puede decir que una función de hash (Gen, h) es resistente a preimagen, si para todo adversario que funciona como un algoritmo aleatorizado de timepo polinomial, existe una función despreciable $f(n)$ tal que:

$$Pr(\text{Adversario gane } HashPreImg(n)) \leq f(n)$$

Ahora, queremos demostrar que si (Gen, h) es resistente a colisiones, entonces (Gen, h) es resistente a preimagen. Vamos a demostrarlo por contrapositivo.

Supongamos que (Gen, h) no es resistente a preimagen. Por ende, existe un adversario que funciona como un algoritmo aleatorizado de tiempo polinomial, tal que para toda función despreciable $f(n)$, se tiene que:

$$Pr(\text{Adversario gane } HashPreImg(n)) \not\leq f(n)$$

Con esta información jugemos $HashCol(n)$ con la siguiente estrategia para el adversario:
- El adversario recibe s

- Genera aleatoriamente un mensaje m de tamaño $n+1$ y calcula $h^s(m)$

- Con el algoritmo de la parte anterior, encuentra m' tal que $h^s(m') = h^s(m)$

- Si $m' \neq m$, retorna el par m', m

- En otro caso, retorna falso (o un par de strings aleatorias)

Notemos que todos los pasos son trivialmente polinomiales bajo el tamaño n, por ende, el algoritmo es polinomial. Veamos cuál es la probabilidad de que el adversario gane.

Dado que la cantidad de mensajes candidatos de tamaño $n+1$ es 2^{n+1} y que el espacio de hashes es de tamaño 2^n, entonces hay como mínimo una cantidad $2^{n+1} - 2^n + 1 = 2^n + 1$ de mensajes que tienen colisiones

entre sí. Es decir, hay una probabilidad mínima de $\frac{2^n+1}{2^{n+1}} \geq \frac{1}{2}$ de sacar un mensaje con colisión.

Supongamos que estamos en la situación en que se sacó un mensaje con colisión. Notar que ahora, para ganar el juego, necesitamos que el algoritmo retorne un m' que cumpla correctamente con tener el mismo hash, y que sea disitnto.

La probabilidad de que cumpla con tener el mismo hash es $Pr(\text{Adversario gane } HashPreImg(n))$. La probabilidad de que no sea distinto es más complejo de calcular.

Notar que para un par de colisiones m, m' tal que $h^s(m) = h^s(m')$, la probabilidad de que el algoritmo retorne algo distinto a m con input $h^s(m)$ o que retorne m' con input $h^s(m)$ debe ser distinta a 0 (ya que si ambas fuera 0, sería una contradicción, ya que implica que se deben retornar 2 outputs en todo caso del algoritmo). Sin pérdida de generalidad, digamos entonces que la probabilidad que retorne algo distinto a m es k (sería equivalente en el caso de m'). Por ende, para todo par que hay de colisiones, en la mitad de ellas (por lo menos) hay una probabilidad k de obtener un resultado distinto (asumiendo que ya ocurrió que el adversario ganó en $HashPreImg(n)$).

Juntando todo, se obtiene que:

$$Pr(\text{Adversario gane } HashCol(n)) \geq \frac{Pr(\text{Adversario gane } P(n))k}{4}$$

Y dado que:

$$Pr(\text{Adversario gane } HashPreImg(n)) \not\leq f(n)$$

$$\frac{Pr(\text{Adversario gane } P(n))k}{4} \not\leq \frac{f(n)k}{4}$$

Por ende, se cumple que

$$Pr(\text{Adversario gane } HashCol(n)) \not\leq \frac{f(n)k}{4}$$

Para toda función despreciable $f(n)$, y dado que $k/4$ es simplemente un factor positivo, es indistinto hablar de toda función de $f(n)$, a toda función $f(n)k/4$ dado que $f(n)$ es despreciable. Por ende:

$$Pr(\text{Adversario gane } HashCol(n)) \not\leq f(n)$$

Por ende, se encontró una estrategia que sirve para el adversario, y entonces, no es resistente a colisiones.

Por contrapositivo, concluimos que si un (Gen, h) es resistente a colisiones, entonces (Gen, h) es resistente a preimagen.