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

IIC3253 — Criptografía y Seguridad Computacional

Sebasthian von Bergen (15635635)

Tarea 1 – Respuesta Pregunta 4

1. Definiendo el juego $Hash - Col(n)$, dada una funcion de hash (Gen, h):

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

    Podemos definir la nocion de resistencia a colisiones donde, dado una funcion de hash h y dos mensajes arbitrarios m_1, $m_2 \in M$, $m_1 \neq m_2$:

    $$\Pr[h(m_1) = h(m_2)] \leq \frac{1}{|H|} \cdot c \quad (1)$$

    Donde H es el espacion de resultados posibles de la funcion de hash h. Por ejemplo, si h lleva un mensaje de largo arbitrario a un string binario de largo 128 entonces, $\frac{1}{|H|} = \frac{1}{2^{128}}$. La constante $c \geq 1$ es un numero subjetivo que representa que tan lejano de una distribucion uniforme puede estar esta probabilidad y aun ser resistente a colision. Si buscamos la perfeccion, se puede definir $c = 1$ lo que impica que la probailidad de colisiones tiene forma de distribucion uniforme.

    Llevando esta idea al juego, podemos decir que una funcion de hash (Gen, h) es resistence a colisiones si la probabilidad de que el adversario gane es despreciable. Como fue visto en clases, asumimos que esta probabilidad es despreciable si, dado un adversario que funciona con un algoritmo aleatorizado de tiempo polinomial, existe una funcion despreciable $f(n)$ tal que:

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

    La definicion de (1) cumple con esta caracteristica. Para una funcion $f(n) = \frac{1}{2^n}$, sabemos que este valor disminuye a una velocidad mucho mayor que cualquier posible que cualquier polinomio.

2. Queremos demostrar que si (Gen, h) es resitente a colisiones, entonces (Gen, h) es resistente a preimagen. La nocion de ser resistente a preimagen implica que, dado un mensaje m_1 es muy dificil encontar otro mensaje m_2 tal que $h(m_1) = h(m_2)$, es decir, es dificil utilizar información entregada por $h(m_1)$ para construir otro mensaje m_2 que tenga el mismo hash.

    Esto es lo mismo que decir que es dificil encontar dos mensajes que tengan colision dada la funcion de hash (Gen, h). Asumiendo que se construye el mensaje m_2 a partir del $h(m_1)$ con una funcion g, decimes que la funcion de hash es resistente a preimagen si:

    $$\Pr[h(m_1) = h(g(m_1))] \leq f(n)$$

Donde $f(n)$ es una funcion despreciable como definimos arriba. Asumiendo que la funcion de hash (Gen, h) es resistente a colisiones, entonces existe esta funcion despreciable que cumple con la propiedad:

$$\Pr[h(m_1) = h(m_2)] \leq f(n)$$

Dado que definimos la resistencia a colisiones permite al adversario elegir los dos mensajes m_1, m_2, podemos decir que incluso en el caso donde $m_2 = g(m_1)$, se cumple la propiedad de que la probabilidad de colision es despreciable. Ya que la resistencia a colisiones es mantiene para mensajes arbitrarios, es lógico que se mantiene para cualquier mensaje construido.