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 2

Sea el esquema criptográfico (Gen, Enc, Dec) definido sobre los espacios $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^n$. Donde además se cumple que:

$$Gen(k) = 0 \text{ si es que el primer bit de } k \text{ es } 0$$

$$Gen(k) = 2^{1-n} \text{ en otro caso}$$

Por demostrar: Este esquema no es una pseudo-random permutation con una ronda, si $3/4$ es considerado como una probabilidad significativamente mayor a a $1/2$.

Primero, necesitamos una estrategia para el adversario. Digamos que ya se lanzó la moneda ($b = 0$ o $b = 1$). La primera decisión del adversiaro va a ser elegir el string $y = 0^n$. A partir de esto obtiene $f(y)$.

Ahora, dado que no tenemos restricciones sobre las capacidades computacionales del adversario, este genera el conjunto:

$$P = \{Enc(k, 0^n) \;\mid\; k \in \mathcal{K} \text{ tal que } Gen(k) \neq 0\}$$

Ahora, si $f(y) \in P$, el adversario responde que $b = 0$ (que se usó el Enc). En caso contrario, el adversario responde que $b = 1$.

Por demostrar: Esta estrategia implica una tasa de éxito $\geq 3/4$.

Notemos que la probabilidad de que gane el adversario la podemos calcular de la siguiente manera:

$$Pr(\text{gane el adversario}) = Pr(\text{gane el adversario} \mid b = 0)Pr(b = 0) + Pr(\text{gane el adversario} \mid b = 1)Pr(b = 1)$$

$$Pr(\text{gane el adversario}) = Pr(\text{gane el adversario} \mid b = 0)/2 + Pr(\text{gane el adversario} \mid b = 1)/2$$

Notar que si es que $b = 0$, entonces se usó alguna llave para encriptar el valor $f(y)$. Es decir, $\exists k \in \mathcal{K}, Gen(k) \neq 0, Enc(k, 0^n) = f(y)$. Por lo tanto, $f(y) \in P$. Según la decisión del adversario, elige entonces $b = 0$, por lo que gana el juego siempre en este caso. Es decir, $Pr(\text{gane el adversario} \mid b = 0) = 1$.

$$Pr(\text{gane el adversario}) = 1/2 + Pr(\text{gane el adversario} \mid b = 1)/2$$

Ahora, si $b = 1$, entonces $f(y)$ distribuye uniforme en $\mathcal{C}$. Veamos el tamaño de P. Dado que por cada clave hay como máximo un elemento de P, se tiene que $|P| \leq |\{k \in \mathcal{K} \text{ tal que } Gen((k) \neq 0\}|$. Por enunciado, la mitad de los elementos de $\mathcal{K}$ cumplen con que tienen alguna probabilidad de ser generados (sólo los que empiezan con el bit 1). Por ende, $|P| \leq |\mathcal{K}|/2 = 2^n/2 = 2^{n-1}$. La probabilidad de que gane el adversario entonces se puede representar como:

$$Pr(\text{gane el adversario} \mid b = 1) = \frac{|C| - |P|}{|\mathcal{C}|}$$

$$Pr(\text{gane el adversario} \mid b = 1) \geq \frac{2^n - 2^{n-1}}{2^n}$$
$$Pr(\text{gane el adversario} \mid b = 1) \geq 1 - 1/2$$
$$Pr(\text{gane el adversario} \mid b = 1) \geq 1/2$$

Por lo tanto:

$$Pr(\text{gane el adversario}) \geq 1/2 + 1/4$$
$$Pr(\text{gane el adversario}) \geq 3/4$$

Por ende, existe una estrategia tal que el adversario tiene una probabilidad considerable de ganar. Por ende, el esquema criptográfico no es una pseudo-random permutation.