PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
ESCUELA DE INGENIERÍA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN

Criptografía y Seguridad Computacional - IIC3253
Tarea 1
Tomás Valenzuela

Pregunta 2

Considere un esquema criptográfico (Gen, Enc, Dec) definido sobre los espacios $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^n$. Suponga además que Gen no permite claves cuyo primer bit sea 0, y que el resto de las claves son elegidas con distribución uniforme. Demuestre que este esquema no es una pseudo-random permutation con una ronda, si $\frac{3}{4}$ es considerada como una probabilidad significativamente mayor a $\frac{1}{2}$.

Respuesta

La estrategia del adversario sería dar un mensaje cualquiera m, y cuando reciba $f(m)$ de vuelta tratar de desencriptar el mensaje con todas las llaves posibles $k_n = Gen(1x)$ para todo x en $\{0,1\}^{n-1}$, si logra encontrar que $f(m) = Enc(k_i, m)$ con i entre 0 y n, entonces elige 1, de otra forma elige 0.

La probabilidad del adversario de ganar es:

Pr(Adversario gana juego) =

$$\Pr(\text{Adversario gana juego} \mid b = 0) \cdot \Pr(b = 0) + \Pr(\text{Adversario gana juego} \mid b = 1) \cdot \Pr(b = 1) =$$

$$\frac{1}{2} \cdot \Pr(\text{Adversario gana juego} \mid b = 0) + \frac{1}{2} \cdot \Pr(\text{Adversario gana juego} \mid b = 1)$$

Por partes:
$\Pr(\text{Adversario gana juego} \mid b = 0) = 1$

Para la otra probabilidad hay que tener en cuenta qué pasa si justo la permutación π elegida cumple que $\pi(m) = Enc(k, m)$ para algún $k \in Gen(1x)$ para todo x en $\{0,1\}^{n-1}$, esto haría que el adversario elija 1 erróneamente.
Además, tenemos el espacio k de todas las llaves posibles de tamaño 2^{n-1} ya que solo están las que empiezan con el bit 1.
$\Pr(\text{Adversario gana juego} \mid b = 1) =$

$$\sum_{i=0}^{2^{n-1}}[\Pr(\pi(m) \neq Enc(k_i, m)] = 1 \text{ - } \sum_{i=0}^{2^{n-1}}[\Pr(\pi(m) = Enc(k_i, m)]$$

Casos totales de permutaciones: $2^n!$
Casos favorables: $2^{n-1}!$ por clave, por lo que queda:

$$1 - \sum_{i=0}^{2^{n-1}} \frac{2^{n-1}!}{2^n!}$$

$$1 - \sum_{i=0}^{2^{n-1}} \frac{1}{2^n}$$

$$1 - \frac{2^{n-1}}{2^n}$$

$$\Pr(\text{Adversario gana juego} \mid b = 1) = 1 - \tfrac{1}{2} = \tfrac{1}{2}$$

Finalmente:

$$\tfrac{1}{2}\cdot \Pr(\text{Adversario gana juego} \mid b = 0) + \tfrac{1}{2}\cdot \Pr(\text{Adversario gana juego} \mid b = 1)$$

$$\tfrac{1}{2} \cdot 1 + \tfrac{1}{2} \cdot \tfrac{1}{2} = \tfrac{3}{4}$$

Esta es la probabilidad que el adversario gane el juego, la cual es significativamente más grande que $\frac{1}{2}$. Entonces, este esquema no es una pseudo-random permutation como se buscaba demostrar.