NOMBRE: Benjamín Farías Valdés

N.ALUMNO: 17642531

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

IIC3253 — Criptografía y Seguridad Computacional — 1' 2022

Tarea 1

Pregunta 2

Se demostrará que **existe un adversario capaz de distinguir entre el esquema y una permutación con una probabilidad mayor o igual a $\frac{3}{4}$**, utilizando el juego entre el verificador y adversario visto en clase.

El **verificador** elegirá con distribución uniforme el valor de $b \in \{0,1\}$. Si b vale 0, entonces obtendrá una llave k según la distribución Gen y definirá $f(x) := Enc(k,x)$ como la función de encriptación. Si b vale 1, entonces definirá $f(x) := \pi(x)$ como la función de encriptación, con $\pi(x)$ una permutación elegida con distribución uniforme.

El **adversario** tendrá precomputada una tabla de tamaño exponencial tal que **dado un** $y \in \mathcal{M}$, contiene los pares $< k, Enc(k,y) >$, donde se tienen todas las posibles llaves $k \in \mathcal{K}$ que son de la forma $k = 1.....$, así como los textos cifrados correspondientes a aplicar el esquema sobre el elemento y con cada una de estas llaves. Dada esta tabla, el adversario utiliza la siguiente estrategia:

1. Elige el y **mencionado anteriormente** y le pide el valor de $f(y)$ al verificador.
2. Usando la tabla, busca el valor de k' tal que $Enc(k', y) = f(y)$.
3. Si **no se encuentra este valor en la tabla** (ya que era de la forma $k' = 0.....$), entonces indica que $b = 1$, es decir, que se está utilizando una permutación.
4. Si **encuentra el valor** (ya que era de la forma $k' = 1.....$), entonces indica que $b = 0$, es decir, que se está utilizando el esquema criptográfico.

La probabilidad de que gane el adversario es la siguiente:

$$Pr(ganar) = Pr(b=0) \cdot Pr(ganar|b=0) + Pr(b=1) \cdot Pr(ganar|b=1)$$

Como el valor real de b se escoge de manera uniforme:

$$Pr(b=0) = Pr(b=1) = \frac{1}{2}$$

Dado que la tabla se calculó con todas las llaves k que son válidas para el esquema, se tiene que para $b = 0$, el valor de $f(y)$ obtenido será encontrado en la tabla del adversario y por tanto **siempre indicará que se utilizó el esquema de manera correcta:**

$$Pr(ganar|b = 0) = 1$$

En caso de que $b = 1$, el valor de $f(y)$ se encontrará en la tabla si es que la permutación **justo entrega un resultado equivalente a usar el esquema con una llave de la forma** $k = 1.....$, causando que el adversario se equivoque al pensar que se aplicó el esquema. Por lo tanto, se calculará la probabilidad de la siguiente forma:

$$Pr(ganar|b = 1) = Pr(\pi(y) \neq Enc(k, y)|k := 1.....)$$

Esto se puede calcular mediante conteo. La cantidad de permutaciones totales es $(2^n)!$. Si se considera sólo una de las llaves $k = 1.....$, entonces los casos favorables corresponderían a fijar un par $< y, \pi(y) = Enc(k, y) >$ y encontrar la cantidad de permutaciones entre los elementos restantes, es decir, $(2^n - 1)!$. Por lo tanto, al considerar a las 2^{n-1} llaves que son de la forma $k = 1.....$ (ya que se fija el primer bit y se reducen a la mitad), se obtienen $(2^n - 1)! \cdot 2^{n-1}$ casos favorables. La probabilidad queda:

$$Pr(ganar|b = 1) = Pr(\pi(y) \neq Enc(k, y)|k := 1.....) = \frac{(2^n - 1)! \cdot 2^{n-1}}{(2^n)!} = \frac{2^{n-1}}{2^n} = \frac{1}{2}$$

Finalmente, al combinar todas las probabilidades anteriores:

$$Pr(ganar) = \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}$$

Tenemos que el adversario puede distinguir entre el esquema y una permutación con una probabilidad **significativamente mayor a** $\frac{1}{2}$, por lo que con tan solo 1 ronda, queda demostrado que este esquema no es una **Pseudo-Random Permutation**.