Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencia de la Computación
Marcelo Arenas — Martin Ugarte

IIC3253 — Criptografía y Seguridad Computacional — Diego Iruretagoyena

Pregunta 2

Denotemos (Gen, Enc, Dec) sobre espacio mensajes M, espacio llaves K, $M = K = C = \{0,1\}^n$.

- (1) Gen no permite claves cuyo primer bit sea 0
- (2) el resto de las claves son elegidas con distribución uniforme

PD (Gen, Enc, Dec) no es una pseudo-random permutation con una ronda si $\frac{3}{4} >> \frac{1}{2}$.

La criptografía moderna involucra el estudio de técnicas matemáticas para asegurar información digital, sistemas y procesos distribuidos en contra de ataques adversarios. Primero, contextualicemos la técnica aprendida en clase para modelar un juego. Queremos formalizar la idea de seguridad y lograr estructurar la idea de un adversario que podría ganar información acerca de la forma en la que se eligen las llaves. Se representa un escenario enmarcado en un juego de turnos que representa nociones de seguridad frente a ataques basados en ganancia de información de parte de un adversario con capacidad computacional infinita. Además, suponemos principios de Kerchoff, en donde todo menos la llave es públicamente conocido.

La estructura del juego visto en clases es el siguiente:

Sean M, K y C espacios de mensajes, llaves t.q. $M = K = C = \{0,1\}^n$ con $1 \leq n$. Para un sistema criptográfico (Enc, Dec) sobre M, K y C, se define el siguiente juego con parámetros $1 \leq r, q$:

- (1) Verificador escoje $b \in 0, 1$ con distribución uniforme.

  (1.1) Si $b = 0 \rightarrow$ Gen distribuye uniforme $K \subseteq K$ tal que $|K| = r$. Luego $f(x) = Enc(k, m)$.

  (1.2) Else, el verificador escoje con distribución uniforme una permutación $\pi : M \rightarrow M$. Luego $f(x) = \pi(m)$.

- (2) Para $i = 1, 2, ..., q$ se realizan los siguientes pasos.

  (2.1) El adversario elije un mensaje $m_i \in M$.

  (2.2) $b = 0$, entonces el verificador responde de la siguiente forma. Si $m_i \neq m_j \forall j \in 1, ..., i1$, entonces el verificador escoje $k \in K$ con distribución uniforme y entrega la respuesta $Enc(k, m_i)$. Si $\exists m_i, m_i = m_j$ para algún $j \in 1, ..., i1$, entrega la misma respuesta que en el paso j.

  (2.3) $b = 1$, entonces el verificador entrega la respuesta $\pi(m_i)$.

- (3) El adversario indica si b = 0 o b = 1, y gana si su elección es correcta.

Ahora, en este juego en particular, nos han agregado información relevante.

- Gen distribuye uniforme para todo bit desde $k[1], ..., k[n-1]$ y $k[0]$ **siempre será igual a 1**. Qué nos permite saber esto ? Cómo podríamos atacar este sistema ? Demostraremos que podemos ganar información relevante acerca de $f(x)$.

Debemos demostrar si este sistema es una r-PRP con $r = 1$. El sistema criptográfico (Enc, Dec) se dice un r-pseudorandom permutation si no existe un adversario que pueda ganar con probabilidad significativamente mayor a $\frac{1}{2}$.

Distribución Pseudo-random
Denotemos U_n distribución uniforme sobre $\{0,1\}^n$, i.e. $U_n = \{t \leftarrow \{0,1\}^n : t\}$.

Decimos que una distribución es pseudo-random si es indistingible de la distribución uniforme. Queremos saber si superamos el benchmark de 50% que entrega la elección aleatoria. El esquema (Gen, Enc, Dec) es una **pseudo-random permutation** si no existe un adversario que pueda ganar el juego con probabilidad significativamente mayor a $\frac{1}{2}$. Si tengo $\frac{1}{2} + \frac{1}{2^{1000}}$ entonces no es significativamente mayor.

Este tipo de juegos nos permite estructurar nociones de seguridad y relacionarlas. Por ejemplo, un esquema criptografico que es perfect secrecy es una PRP. No toda PRP tienen propiedad perfect secrecy. **También sabemos que si el espacio de llaves es menor al espacio de mensajes, no puedo tener perfect secrecy**.

Cuáles son las capacidades del adversario ? No imponemos restricciones en las capacidades computacionales del adversario. Definimos qué significa que la probabilidad de ganar el juego sea significativamente mayor a $\frac{1}{2}$. i.e. $\frac{3}{4}$. También tenemos que indicar cuál es el número de rondas Q. Se propone el siguiente ataque suponiendo $Q = 1$.

Como el primer bit siempre es 1, las permutaciones de llaves posibles son (2^{n-1}). Esto es fácil de ver con ejemplos incrementales, por ejemplo si $n = 1$, solo podría encriptar con $k = 1$, si $n = 2$, sería 11 o 10, $n = 3$ sería 111, 110, 101, 100 y así continuando siguiendo la fórmula (2^{n-1}).

Esto es bastante conveniente. Significa que el espacio de llaves de Gen es más pequeño que el de la permutación, **hay mensajes cifrados** $c = Enc(k, y)$ **que serán exclusivos de la permutación**. Además, para $n = 1$, podemos saber inmediatamente al revisar $c[0]$, por lo que se puede ganar información en este caso al revisar el primer bit.

- Adversario elige $y = 0^n$.
- Recibimos resultado $f(y) = c$.
- Observamos $c[0]$ y si el mensaje cifrado es computable por algún $k \in 1||2^{n-1}$ (llave en el espacio de llaves con primer bit igual a 1)

Existe la posibilidad que haya sido una respuesta que se encuentra en el espacio compartido. Si $\pi(y) = Enc(k, y)$, el adversario da la respuesta equivocada. Esa probabilidad es equivalente a:

$$PR(\pi(y) \neq Enc(k, m))$$

$$= 1 - PR(\pi(y) = Enc(k, m))$$

Calculamos probabilidad de ganar.
$Pr(\text{Adversario gana el juego } |b = 0) * Pr(b = 0) + Pr(\text{Adversario gana el juego } |b = 1) * Pr(b = 1) =$

$PR(\pi(y) = Enc(k, m)) = \dfrac{(2^{n-1})!}{(2^n)!} = \dfrac{1}{2}$

$PR(\pi(y) \neq Enc(k, m)) = 1 - \dfrac{1}{2}$

Entonces,

$Pr(\text{Adversario gana el juego } |b = 0) * Pr(b = 0) + Pr(\text{Adversario gana el juego } |b = 1) * Pr(b = 1) =$

$$n = 1|1 * \frac{1}{2} + \frac{1}{2} * \frac{1}{2} = \frac{3}{4}$$

Al ser 75% considerada una probabilidad significativamente mayor al benchmark de la uniformidad de elección, podemos concluir que esto no es una r-PRP con $r = 1$.