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

Ayudante: Nicholas Mc-Donnell
Email: `namcdonnell@uc.cl`

Ayudantía 08

Teorema Esquema PRG

IIC3253 – Criptografía

Fecha: 2021-05-19

1. Recordatorio

Definición 1.1 (Generador Pseudo-Aleatorio (PRG)). Sea $\ell(\cdot)$ un polinomio y sea G un algoritmo determinista en `P-TIME` tal que para toda entrada $s \in \{0,1\}^n$, G devuelve un string de largo $\ell(n)$. Se dice que G es PRG si:

1) (Expansión): $\forall n\, \ell(n) > n$.

2) (Pseudo-Aleatoriedad): Para todo distinguidor en `RP-TIME` D se tiene que existe una función despreciable f tal que:

$$\left| \underset{r \leftarrow \{0,1\}^{\ell(n)}}{P}[D(r) = 1] - \underset{s \leftarrow \{0,1\}^n}{P}[D(G(s)) = 1] \right| \leq f(n)$$

Definición 1.2 (Esquema de Cifrado Basado en PRG). Sea G un PRG con factor de expansión ℓ. Se define el esquema de cifrado de llave privada para mensajes de largo $\ell(n)$ a continuación:

- `Gen`: dado 1^n, elige $k \leftarrow \{0,1\}^n$ de forma uniformemente aleatoria.

- `Enc`: dado una llave $k \in \{0,1\}^n$ y un mensaje $m \in \{0,1\}^{\ell(n)}$, retorna el texto cifrado

$$c := G(k) \oplus m.$$

- `Dec`: dado una llave $k \in \{0,1\}^n$ y un texto cifrado $c \in \{0,1\}^{\ell(n)}$, retorna el mensaje

$$m := G(k) \oplus c.$$

Definición 1.3 (Cifrado Indistinguible ante Ataque de Texto Cifrado)**.** Dado `Enc` se define el siguiente juego:

1) El Adversario elige $m_0, m_1 \in \{0,1\}^{\ell(n)}$.

2) El Verificador elige $b \in \{0,1\}$ y le devuelve a $\texttt{Enc}(k, m_b)$ al Adversario.

3) El Adversario indica si $b = 0$ o $b = 1$.

Si $P(A) \leq \frac{1}{2} + f(n)$, donde A es el evento que el Adversario gane y f es una función despreciable, se dice que `Enc` es un cifrado indistinguible ante un ataque de texto cifrado.

Teorema 1.1. *Dado un PRG, G, se tiene que el esquema basado en G, $(\texttt{Gen}, \texttt{Enc}, \texttt{Dec})$, tiene cifrado indistinguible ante un ataque de texto cifrado,*

Demostración. Se usará contrapositiva para demostrar el teorema. Se denota $\Pi = (\texttt{Gen}, \texttt{Enc}, \texttt{Dec})$. Sea A el algoritmo en `RP-TIME` tal que $P(A_{wins}) > \frac{1}{2} + f(n)$ para toda función despreciable f y donde A_{wins} es el evento donde el algoritmo A gana el juego de la definición 1.3. Se define $\varepsilon(n) := P(A_{wins}) - \frac{1}{2}$, y se nota que ε no es una función despreciable[1]. Con lo anterior se construye un algoritmo distinguidor D:

Distinguidor D
La entrada es $w \in \{0,1\}^{\ell(n)2}$. 1) Se toman dos mensajes al azar $m_0, m_1 \in \{0,1\}^{\ell(n)}$. 2) Se elige $b \in \{0,1\}$ al azar. Se define $c := w \oplus m_b$. 3) Se define $b' := A(c)$. Retorna 1 si $b' = b$, y 0 en otro caso.

Dado D se quiere calcular $\underset{s \leftarrow \{0,1\}^n}{P}[D(G(s)) = 1]$ y $\underset{r \leftarrow \{0,1\}^{\ell(n)}}{P}[D(r) = 1]$. Para el primer cálculo, se nota que la probabilidad corresponde a la probabilidad de que A gane el juego de la definición 1.3 con el esquema Π, por lo que $\underset{s \leftarrow \{0,1\}^n}{P}[D(G(s)) = 1] = \frac{1}{2} + \varepsilon(n)$. Para el segundo cálculo, se nota que la probabilidad corresponde a $\frac{1}{2}$ ya que corresponde a la

[1] $P(A_{wins}) \leq \varepsilon(n) = \frac{1}{2}$.

[2] Se asume que n es determinable desde $\ell(n)$.

probabilidad de que A gane el juego de la definición 1.3 con el esquema de OTP. Por lo que $\left| \underset{r \leftarrow \{0,1\}^{\ell(n)}}{P}[D(r) = 1] - \underset{s \leftarrow \{0,1\}^{n}}{P}[D(G(s)) = 1] \right| = \varepsilon(n)$, y con eso se tiene que G no es PRG. $\square$