Clase 5: “one-time-pad” pseudoaleatorio

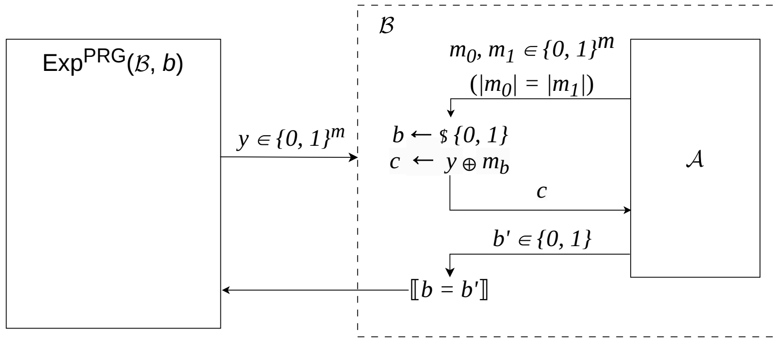
Fernando Virdia, versión: 0.0.1, junio 2024

Lemma 4 *Sea G un (ε, t)-PRG. Un PR-OTP Π^G que utiliza G, otorga (ε', t')-secrecy con $\varepsilon' = 2\varepsilon$ y $t' \approx t$.*

Demostración. Supongamos de haber encontrado un adversario $\mathcal{A}$ que corre en tiempo $\leq t'$ y que tiene ventaja $\mathsf{Adv}(\mathsf{Exp}^{\mathrm{OTS}}, \mathcal{A}) > \varepsilon'$ cuando “juega”. A partir de $\mathcal{A}$ construiremos $\mathcal{B}$ que corre en tiempo $t \approx t'$ y que juega $\mathsf{Exp}^{\mathrm{PRG}}$.

$\mathcal{B}(y \in \{0,1\}^m)$

1 : $b \xleftarrow{\$} \{0,1\}$
2 : $m_0, m_1, \sigma \leftarrow \mathcal{A}_1()$
3 : $c \leftarrow y \oplus m_b$
4 : $b' \leftarrow \mathcal{A}_2(c, \sigma)$
5 : **return** $[\![b = b']\!]$



Calculemos $\mathsf{Adv}(\mathsf{Exp}^{\mathrm{PRG}}, \mathcal{B})$:

- Si $\mathcal{B}$ recibe $y \leftarrow G(s)$ en $\mathsf{Exp}^{\mathrm{PRG}}$, internamente crea para $\mathcal{A}$ el mismo ambiente de la versión “bit-guessing” de $\mathsf{Exp}^{\mathrm{OTS}}$. Por lo tanto,

$$\Pr[\mathsf{Exp}^{\mathrm{PRG}}(\mathcal{B}, 0) \Rightarrow 1] = \Pr[\overline{\mathsf{Exp}^{\mathrm{OTS}}_{\Pi^G}}(\mathcal{A}) \Rightarrow 1].$$

- Si $\mathcal{B}$ recibe $y \xleftarrow{\$} \{0,1\}^m$, simula nuevamente $\overline{\mathsf{Exp}^{\mathrm{OTS}}}$ para $\mathcal{A}$, pero en este caso es con un cifrado OTP!

$$\Pr[\mathsf{Exp}^{\mathrm{PRG}}(\mathcal{B}, 1) \Rightarrow 1] = \Pr[\overline{\mathsf{Exp}^{\mathrm{OTS}}_{\mathrm{OTP}}}(\mathcal{A}) \Rightarrow 1].$$

Abusando la notación, sea $b' \leftarrow \mathcal{A}_2(c \leftarrow y \oplus m_b)$ y repliquemos la demostración de Lemma 3, para obtener

$$\begin{aligned}
\forall b \quad \Pr[\mathsf{Exp}^{\mathrm{PRG}}(\mathcal{B}, 1) \Rightarrow 1] &= \Pr[b' \Rightarrow b] \\
&= \frac{1}{2}\Big(\Pr[b' = b \mid b = 0] + \Pr[b' = b \mid b = 1]\Big) \\
&= \frac{1}{2} + \frac{1}{2}\Big(\Pr[b' = 1 \mid b = 1] - \Pr[b' = 1 \mid b = 0]\Big).
\end{aligned}$$

Dado que $y \sim U(\{0,1\}^m)$,[4] $y \oplus m_0 \sim y \oplus m_1 \sim U(\{0,1\}^m)$.[5] De acuerdo, las variables aleatorias $\mathcal{A}_2(y \oplus m_0)$ y $\mathcal{A}_2(y \oplus m_1)$ tienen la misma distribución.

$$\begin{aligned}
\Pr_y[\mathcal{A}_2(y \oplus m_0; R) = b \mid R = r] &= \Pr[(y \oplus m_0) \in \mathcal{A}_2^{-1}(b) \mid R = r] \\
&= \sum_{c \in \in \mathcal{A}_2^{-1}(b) | R = r} \Pr_y[c = y \oplus m_0] \\
&= \sum_{c \in \in \mathcal{A}_2^{-1}(b) | R = r} \Pr_y[c = y \oplus m_1] \\
&= \Pr[(y \oplus m_1) \in \mathcal{A}_2^{-1}(b) \mid R = r] \\
&= \Pr_y[\mathcal{A}_2(y \oplus m_1; R) = b \mid R = r].
\end{aligned}$$

[4] O equivalentemente, como corolario del secreto perfecto del OTP.

[5] $y \oplus m_0$ y $y \oplus m_1$ *no son independientes*, pero tienen la misma distribución. $\mathcal{A}_2$ nunca ve ambas variables al mismo tiempo.

Sigue que,

$$\begin{aligned}\Pr[b' = 1 \mid b = 1] &= \Pr[\mathcal{A}_2(y \oplus m_1) = 1] \\ &= \Pr[\mathcal{A}_2(y \oplus m_0) = 1] \\ &= \Pr[b' = 1 \mid b = 0],\end{aligned}$$

y por lo tanto $\Pr[\mathsf{Exp}^{\mathrm{PRG}}(\mathcal{B}, 1) \Rightarrow 1] = \frac{1}{2}$, y

$$\begin{aligned}\varepsilon \geq \mathsf{Adv}(\mathsf{Exp}^{\mathrm{PRG}}, \mathcal{B}) &= \left|\Pr[\mathsf{Exp}^{\mathrm{PRG}}(\mathcal{B}, 0) \Rightarrow 1] - \Pr[\mathsf{Exp}^{\mathrm{PRG}}(\mathcal{B}, 1) \Rightarrow 1]\right| \\ &= \left|\Pr[\overline{\mathsf{Exp}^{\mathrm{OTS}}}(\mathcal{A}) \Rightarrow 1] - \frac{1}{2}\right| \\ &= \mathsf{Adv}(\overline{\mathsf{Exp}^{\mathrm{OTS}}}, \mathcal{A}) = \frac{1}{2}\mathsf{Adv}(\mathsf{Exp}^{\mathrm{OTS}}, \mathcal{A}) > \frac{\varepsilon'}{2},\end{aligned}$$

dado que por suposición G es un (ε, t)-PRG. Claramente, $t' \approx t$ y $\varepsilon' < 2\varepsilon$. Por lo tanto PR-OTP otorga $(\varepsilon' = 2\varepsilon, t' \approx t)$-secrecy. $\square$

Comentario 17 *Otorgar $(\varepsilon' = 2\varepsilon, t' \approx t)$-secrecy quiere decir que un atacante contra Π^G tiene al máximo doble de la ventaja de un atacante contra G. En términos de bit-security,* $\log_2(\frac{t}{2\varepsilon}) = \log_2(\frac{t}{\varepsilon}) - 1$, i.e. *solamente "un bit" de seguridad es perdido.*

Si quisiéramos determinar la seguridad concreta en bits, necesitaríamos una construcción concreta de G, la cual determinaría (ε, t).

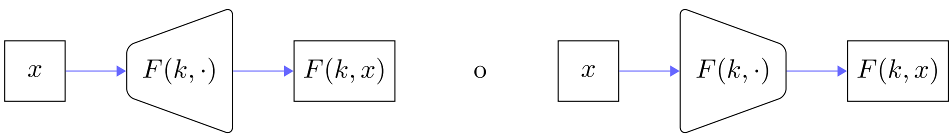
Ahora vamos a ver dos primitivas relacionadas al PRG, utilizadas para construir PRGs y mas.

Definición 10 (PRF) *Sean $\mathcal{K}$, $\mathcal{R}$ dos conjuntos finitos, $\mathcal{D}$ un conjunto. Sea $F \colon \mathcal{K} \times \mathcal{D} \to \mathcal{R}$ una función implementable como algoritmo determinista eficiente.*

$\mathsf{Exp}^{\mathrm{PRF}}(\mathcal{A}, b)$	$R(x)$
$1: \; k \xleftarrow{\$} \mathcal{K}$	$1: \; \textbf{if } x \notin L:$
$2: \; L \leftarrow [\,]$	$2: \quad y \xleftarrow{\$} \mathcal{R}$
$3: \; \textbf{if } b = 0 : \mathcal{O}(\cdot) \leftarrow F(k, \cdot)$	$3: \quad L[x] \leftarrow y$
$4: \; \textbf{else } : \mathcal{O}(\cdot) \leftarrow R(\cdot)$	$4: \; \textbf{return } L[x]$
$5: \; b' \leftarrow \mathcal{A}^{\mathcal{O}(\cdot)}()$	
$6: \; \textbf{return } b'$	

Decimos que F es una familia de funciones (ε, t, q)-pseudoaleatoria indexada por $k \in \mathcal{K}$ (PRF, "pseudorandom function family"), si dado cualquier adversario $\mathcal{A}$ que corre en tiempo $\leq t$ y hace $\leq q$ queries (consultas) a $\mathcal{O}(\cdot)$, tiene ventaja

$$\mathsf{Adv}(\mathsf{Exp}^{\mathrm{PRF}}, \mathcal{A}) := \left|\Pr[\mathsf{Exp}^{\mathrm{PRF}}(\mathcal{A}, 0) \Rightarrow 1] - \Pr[\mathsf{Exp}^{\mathrm{PRF}}(\mathcal{A}, 1) \Rightarrow 1]\right| \leq \varepsilon.$$



Comentario 18 *Bajo el perfil teórico, un PRG requiere un input aleatorio, y retorna un solo output pseudoaleatorio. Una PRF $F(k, \cdot) \colon \mathcal{D} \to \mathcal{R}$ tolera q inputs $x_i \in \mathcal{D}$ no necesariamente aleatorios, retornando siempre output pseudoaleatorio.*