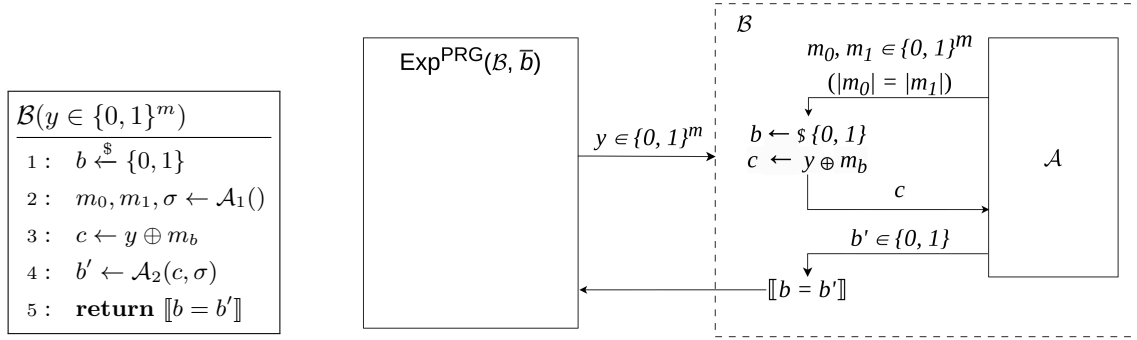


Clase 5: “one-time-pad” pseudoaleatorio

Fernando Virdia, versión: 0.1, mayo 2025

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 $t' \approx t$.

Proof. Supongamos de haber encontrado un (ε', t') -atacante: o sea un adversario $\mathcal{A}$ que corre en tiempo $\leq t'$ y que tiene ventaja $\text{Adv}(\text{Exp}^{\text{OTS}}, \mathcal{A}) > \varepsilon'$ cuando “juega” Exp^{OTS} . A partir de $\mathcal{A}$ construiremos $\mathcal{B}$ que corre en tiempo $t \approx t'$ y que juega Exp^{PRG} .



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

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

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

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

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

Por definicion del OTP, la distribucion de $y \oplus m_0$ y la de $y \oplus m_1$ son identicas, uniformes en $\mathcal{C}$. Abusando la notación, sea $b' \leftarrow \mathcal{A}_2(\sigma, c \leftarrow y \oplus m_b; r)$, donde σ es independiente de b (el bit mostrado internamente por $\mathcal{B}$), así como lo son las monedas $r \sim U(R)$, y repliquemos la demostración de Lemma 3, para obtener

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

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.

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

⁴O 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 $\Pr[\text{Exp}^{\text{PRG}}(\mathcal{B}, 1) \Rightarrow 1] = \frac{1}{2}$, y

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

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

Comentario 18. 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) .

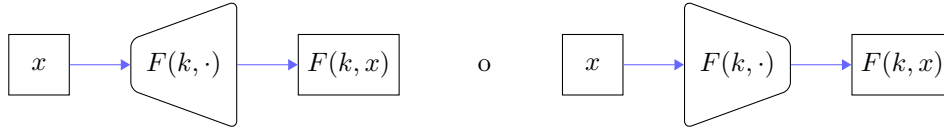
Ahora vamos a ver dos primitivas relacionadas al PRG, utilizadas para construir PRGs y mas.

Definición 13 (PRF). Sean $\mathcal{K}$, $\mathcal{R}$ y $\mathcal{D}$ conjuntos finitos. Sea $F: \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{R}$ una función implementable como algoritmo determinista eficiente.

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

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

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



Comentario 19. Bajo el perfil teórico, un PRG requiere un input aleatorio, y retorna un solo output pseudoaleatorio. Una PRF $F(k, \cdot): \mathcal{D} \rightarrow \mathcal{R}$ tolera q inputs $x_i \in \mathcal{D}$ no necesariamente aleatorios, retornando siempre output pseudoaleatorio.