

Clase 7: PRP $\Rightarrow$ PRF

Fernando Virdia, versión: 0.1, mayo 2025

Lemma 7 (PRP-PRF switching lemma). Sea $\pi: \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{D}$ una (ε, t, q) -PRP. Entonces π es una (ε', t', q') -PRF con $t' = t$, $q' = q$, $\varepsilon' = \varepsilon + \frac{q(q-1)}{2|\mathcal{D}|}$.

Proof. Supongamos que $\mathcal{A}$ sea un adversario contra π usado como una PRF con $\mathcal{R} = \mathcal{D}$, y que evalúa $\mathcal{O}(\cdot)$ sobre inputs distintos, sin pérdida de generalidad. Observando $\text{Exp}^{\text{PRF}}(\mathcal{A}, 0)$ y $\text{Exp}^{\text{PRP}}(\mathcal{A}, 0)$, notamos que del punto de vista de $\mathcal{A}$ son experimentos idénticos si $F = \pi$ en Exp^{PRF} ,

$$\Rightarrow \Pr[\text{Exp}^{\text{PRF}}(\mathcal{A}, 0) \Rightarrow 1] = \Pr[\text{Exp}^{\text{PRP}}(\mathcal{A}, 0) \Rightarrow 1].$$

Calculamos,

$$\begin{aligned} \text{Adv}(\text{Exp}^{\text{PRF}}, \mathcal{A}) &= \left| \Pr[\text{Exp}^{\text{PRP}}(\mathcal{A}, 0) \Rightarrow 1] - \Pr[\text{Exp}^{\text{PRF}}(\mathcal{A}, 1) \Rightarrow 1] \right| \\ &= \left| \Pr[\text{Exp}^{\text{PRP}}(\mathcal{A}, 0) \Rightarrow 1] - \underbrace{\Pr[\text{Exp}^{\text{PRP}}(\mathcal{A}, 1) \Rightarrow 1] + \Pr[\text{Exp}^{\text{PRP}}(\mathcal{A}, 1) \Rightarrow 1]}_{=0} - \Pr[\text{Exp}^{\text{PRF}}(\mathcal{A}, 1) \Rightarrow 1] \right| \\ &\leq \text{Adv}(\text{Exp}^{\text{PRP}}, \mathcal{A}) + \left| \Pr[\text{Exp}^{\text{PRP}}(\mathcal{A}, 1) \Rightarrow 1] - \Pr[\text{Exp}^{\text{PRF}}(\mathcal{A}, 1) \Rightarrow 1] \right|. \quad (\text{por desig. triangular}) \end{aligned}$$

Ahora notamos que $\text{Exp}^{\text{PRP}}(\mathcal{A}, 1)$ y $\text{Exp}^{\text{PRF}}(\mathcal{A}, 1)$ son idénticos desde el punto de vista de $\mathcal{A}$, mientras tanto que el siguiente evento no sucede:

$$Z = “\exists i, j \in [q] : i \neq j \wedge R(x_i) = R(x_j) \text{ durante } \text{Exp}^{\text{PRF}}(\mathcal{A}, 1)”$$

Usando el lema de la diferencia,

$$\left| \Pr[\text{Exp}^{\text{PRP}}(\mathcal{A}, 1) \Rightarrow 1] - \Pr[\text{Exp}^{\text{PRF}}(\mathcal{A}, 1) \Rightarrow 1] \right| \leq \Pr[Z].$$

Dado que $R(\cdot)$ muestrea $U(\mathcal{R}) = U(\mathcal{D})$ de manera independiente si los inputs son distintos (en cuanto π es una PRP), por la paradoja del cumpleaños $\Pr[Z] \leq \frac{q(q-1)}{2|\mathcal{R}|}$, y de consecuencia

$$\text{Adv}(\text{Exp}^{\text{PRF}}, \mathcal{A}) \leq \text{Adv}(\text{Exp}^{\text{PRP}}, \mathcal{A}) + \frac{q(q-1)}{2|\mathcal{D}|}.$$

□

Comentario 24. El PRP-PRF switching lemma nos permite construir una PRF con $\mathcal{R} = \mathcal{D}$. Existen construcciones con $\mathcal{R} \neq \mathcal{D}$, como la PRF “GGM”.

Comentario 25. Este tipo de diferencia en ventaja en función de número de queries implica a menudo la necesidad de limitar la duración de las claves secretas usadas. Si en este caso $q \approx \sqrt{\mathcal{D}}$ permitiría distinguir una PRP de una PRF. A menudo esto implica concretamente ataques concretos, como <https://sweet32.info>.

Lemma 8 (PRF $\Rightarrow$ PRG). Sea F una (ε, t, q) -PRF con $\mathcal{R} = \{0, 1\}^r$. Sean $x_1, \dots, x_q \in \mathcal{D}$ elementos distintos ($x_i \neq x_j, \forall i \neq j$). Definimos $G: \mathcal{K} \rightarrow \{0, 1\}^{r \cdot q}$,

$\begin{aligned} &G(k \in \mathcal{K}) \\ &1: \quad \textbf{for } i = 1, \dots, q: \\ &2: \quad \quad y_i \leftarrow F(k, x_i) \\ &3: \quad \textbf{return } y_1 \dots y_q \end{aligned}$

G es un (ε', t') -PRG con $\varepsilon' = \varepsilon$, $t' \approx t$.

Proof. Supongamos un adversario $\mathcal{A}$ que juega $\text{Exp}^{\text{PRG}}(\mathcal{A}, b)$. Sea $\mathcal{B}$ el siguiente adversario contra la PRF.

$\mathcal{B}^{\mathcal{O}}$
1 : for $i = 1, \dots, q$:
2 : $y_i \leftarrow \mathcal{O}(x_i)$
3 : $b' \leftarrow \mathcal{A}(y_1 \dots y_q)$
4 : return b'

Si $b = 1$ en Exp^{PRF} , $\mathcal{O}(\cdot) = \mathcal{R}(\cdot)$,

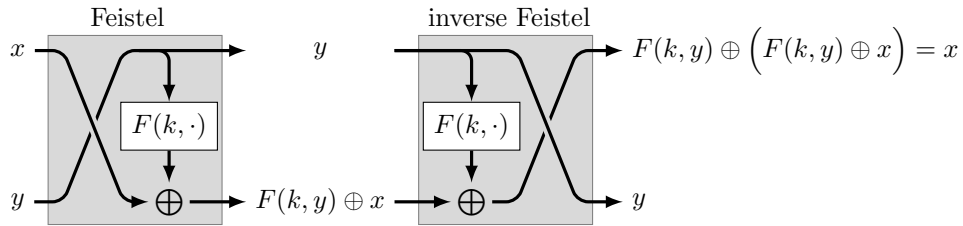
$$\begin{aligned} &\Rightarrow y_i \sim U(\{0, 1\}^r) \\ &\Rightarrow y \sim U(\{0, 1\}^{r \cdot q}) \\ &\Rightarrow \Pr[\text{Exp}^{\text{PRF}}(\mathcal{B}, 1) \Rightarrow 1] = \Pr[\text{Exp}^{\text{PRG}}(\mathcal{A}, 1) \Rightarrow 1]. \end{aligned}$$

Si $b = 0$, $\mathcal{O}(\cdot) = F(k, \cdot)$ con $k \sim U(\mathcal{K})$,

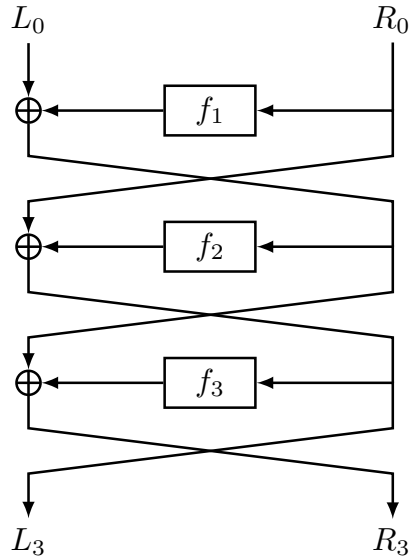
$$\begin{aligned} &\Rightarrow y_i = F(k, x_i) \\ &\Rightarrow y = G(k) \\ &\Rightarrow \Pr[\text{Exp}^{\text{PRF}}(\mathcal{B}, 0) \Rightarrow 1] = \Pr[\text{Exp}^{\text{PRG}}(\mathcal{A}, 0) \Rightarrow 1]. \end{aligned}$$

Sigue que $\text{Adv}(\text{Exp}^{\text{PRG}}, \mathcal{A}) = \text{Adv}(\text{Exp}^{\text{PRF}}, \mathcal{B})$, y claramente $t' \approx t$. $\square$

No vamos a ver GGM y Feistel en detalle, dado que las demostraciones se vuelven bastante difíciles.



(a) Una ronda de Feistel, junto a su inversa.



(b) Múltiples rondas.

Figure 4: PRF $\Rightarrow$ PRP: Feistel network. Imágenes adaptadas de [Ros21, Constructions 6.9, 6.11], usadas con permiso del autor.

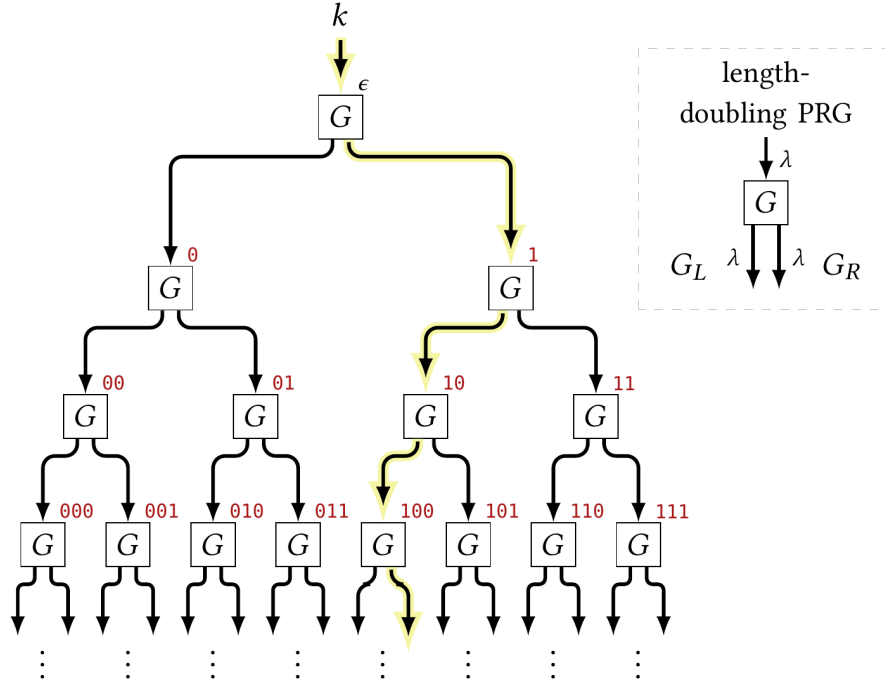


Figure 5: PRG $\Rightarrow$ PRF: construcción GGM (Goldreich-Goldwasser-Micali). Credito de imagen: [Ros21].

Comentario 26. No toda combinación de primitivos otorga seguridad. Por que lo siguiente no funciona?

- Sea G un PRG. $F(k, x) := G(k) \oplus x$ no es una PRF.
- Sea F una PRF. $G(k) := F(1, k) || \dots || F(q, k)$ no es (necesariamente) un PRG.
- Sea G un PRG. $G'(k) := G(k) || G(k)$ no es un PRG.
- Sea G un PRG. $G'(k_1 || k_2) := G(k_1) \wedge G(k_2)$ no es un PRG.

Un resumen:

Inicialmente empezamos con el OTP: secreto perfecto, pero $|k| = |m|$.

Introducimos PRG/PRF/PRP: (ϵ, t) -secrecy, pero $|k| < |m|$.

Aun tenemos dos problemas:

- No podemos cifrar mas de un mensaje: $c_1 \oplus c_2 = m_1 \oplus m_2$.
- No podemos garantizar la integridad de los mensajes: $\text{Dec}(k, c \oplus \Delta) = m \oplus \Delta$.

Usando PRFs, podemos resolver ambos.