Clase 7: PRP ⇒ PRF

Fernando Virdia, versión: 0.0.1, junio 2024

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

Demostración. 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 perdida de generalidad. Observando $\mathsf{Exp}^{\mathrm{PRF}}(\mathcal{A},0)$ y $\mathsf{Exp}^{\mathrm{PRP}}(\mathcal{A},0)$, notamos que del punto de vista de $\mathcal{A}$ son experimentos idénticos si $F=\pi$ en $\mathsf{Exp}^{\mathrm{PRF}}$,

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

Calculamos,

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

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

$$Z=\text{“}\exists i\neq j : R(x_i)=R(x_j) \text{ durante } \mathsf{Exp}^{\mathrm{PRF}}(\mathcal{A},1)''$$

Usando el *lema de la diferencia*,

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

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

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

□

Comentario 23 *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 24 *Este tipo de diferencia en ventaja en función de numero de queries implica a menudo la necesidad de limitar la durada 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 ⇒ PRG) *Sea F una (ε,t,q)-PRF con $\mathcal{R}=\{0,1\}^r$. Sean $x_1,\ldots,x_q\in\mathcal{D}$ elementos distintos ($x_i\neq x_j,\forall i\neq j$). Definimos $G\colon\mathcal{K}\to\{0,1\}^{r\cdot q}$,*

$G(s\in\mathcal{K})$	
1 :	**for** $i=1,\ldots,q$:
2 :	$\quad y_i\leftarrow F(k,x_i)$
3 :	**return** $y_1\|\|\cdots\|\|y_q$

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

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

$\mathcal{B}^{\mathcal{O}}$

1 : **for** $i = 1, \ldots, q$:
2 : $\quad y_i \leftarrow \mathcal{O}(x_i)$
3 : $b' \leftarrow \mathcal{A}(y_1 || \cdots || y_q)$
4 : **return** b'

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

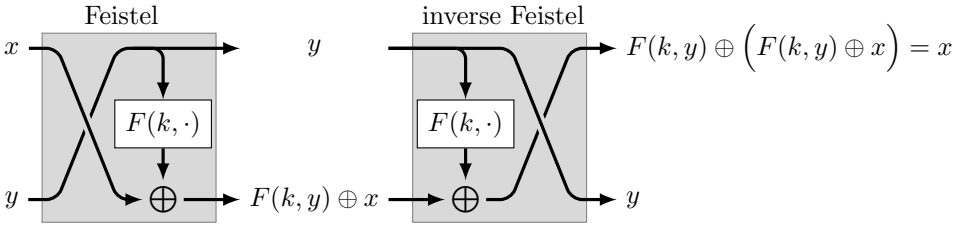
$$\begin{aligned} &\implies y_i \sim U(\{0,1\}^r) \\ &\implies y \sim U(\{0,1\}^{r \cdot q}) \\ &\implies \Pr[\mathsf{Exp}^{\mathrm{PRF}}(\mathcal{B}, 1) \Rightarrow 1] = \Pr[\mathsf{Exp}^{\mathrm{PRG}}(\mathcal{A}, 1) \Rightarrow 1]. \end{aligned}$$

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

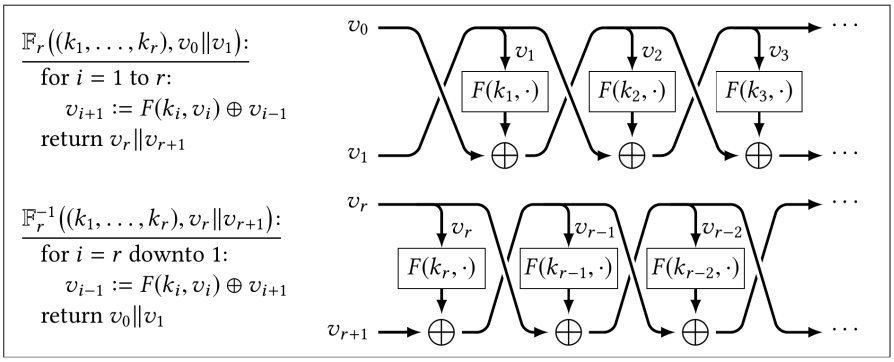
$$\begin{aligned} &\implies y_i = F(k, x_i) \\ &\implies y = G(k) \\ &\implies \Pr[\mathsf{Exp}^{\mathrm{PRF}}(\mathcal{B}, 0) \Rightarrow 1] = \Pr[\mathsf{Exp}^{\mathrm{PRG}}(\mathcal{A}, 0) \Rightarrow 1]. \end{aligned}$$

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

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 ⇒ PRP: Feistel network. Imagenes adaptadas de [Ros21, Constructions 6.9, 6.11], usadas con permiso del autor.

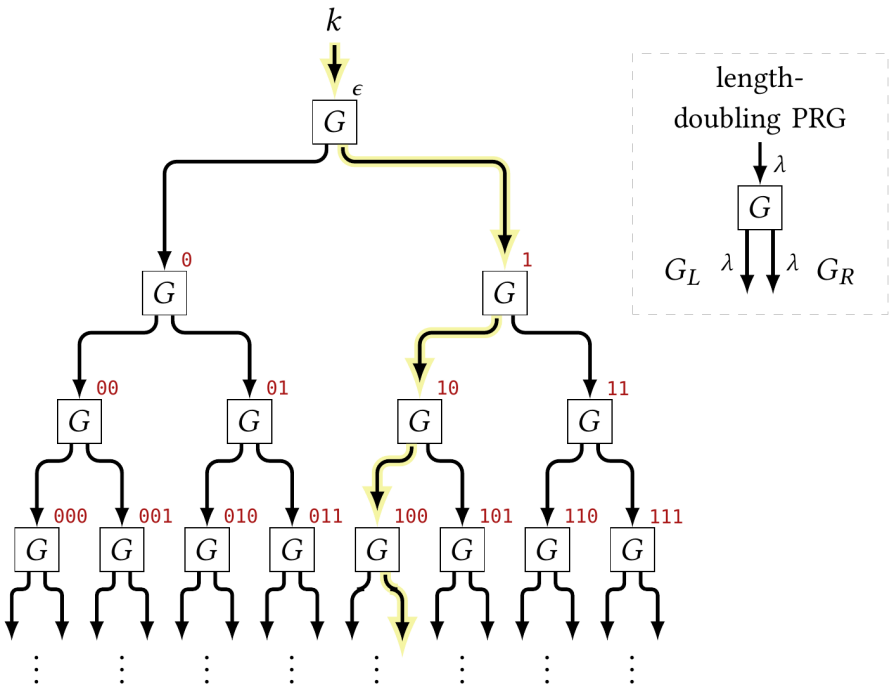


Figure 5: PRG $\Rightarrow$ PRF: construcción GGM (Goldreich-Goldwasser-Micali). Credito de imagen: [Ros21].

Comentario 25 *No toda combinación de primitivos otorga seguridad. Por que lo siguiente no funciona?*

- *Sea G un PRG. $F(k,x) \coloneqq G(k) \oplus x$ no es una PRF.*
- *Sea F una PRF. $G(k) \coloneqq F(1,k)||\cdots||F(q,k)$ no es (necesariamente) un PRG.*
- *Sea G un PRG. $G'(k) \coloneqq G(k)||G(k)$ no es un PRG.*
- *Sea G un PRG. $G'(k_1||k_2) \coloneqq G(k_1) \wedge G(k_2)$ 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: $\mathsf{Dec}(k, c \oplus \Delta) = m \oplus \Delta$.

Usando PRFs, podemos resolver ambos.