Clase 6: cifrados de bloque

Fernando Virdia, versión: 0.0.1, junio 2024

Definición 11 (PRP) *Sean $\mathcal{K}$, $\mathcal{D}$ dos conjuntos finitos. Sea $\pi\colon \mathcal{K}\times\mathcal{D}\to\mathcal{D}$ una función, tal que $\forall k\in\mathcal{K}$, $\pi(k,\cdot):\mathcal{D}\to\mathcal{D}$ tiene una inversa $\pi^{-1}(k,\cdot):\mathcal{D}\to\mathcal{D}$ (tal que $\forall x\in\mathcal{D}, \pi(k,\pi^{-1}(k,x))=\pi^{-1}(k,\pi(k,x))=x$). Sean π y π^{-1} implementables como algoritmos deterministas eficientes.*

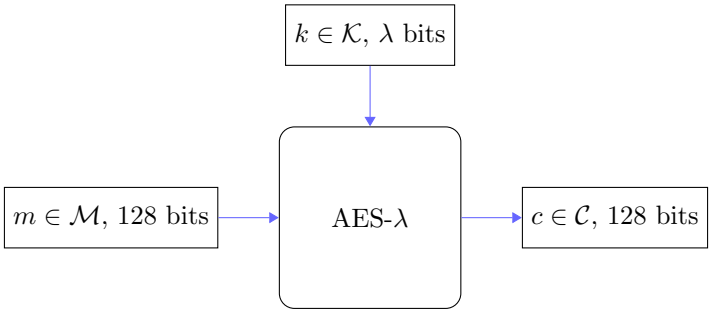
$\mathsf{Exp}^{\mathrm{PRP}}(\mathcal{A},b)$	$P(x)$
$k \xleftarrow{\$} \mathcal{K}$	**if** $x\notin L$:
$L\leftarrow[\,]$	$\quad y \xleftarrow{\$} \mathcal{D}\backslash\{L[x] \mid \forall x\in L\}$
if $b=0:\mathcal{O}(\cdot)\leftarrow\pi(k,\cdot)$	$\quad L[x]\leftarrow y$
else $:\mathcal{O}(\cdot)\leftarrow P(\cdot)$	**return** $L[x]$
$b'\leftarrow\mathcal{A}^{\mathcal{O}(\cdot)}()$	
return b'	

Decimos que π es una familia de permutaciones (ε,t,q)-pseudoaleatoria indexada por $k\in\mathcal{K}$ (PRP, "pseudorandom permutation family"), o un cifrado de bloques, si dado cualquier adversario $\mathcal{A}$ que corre en tiempo $\leq t$ y hace $\leq q$ queries a $\mathcal{O}(\cdot)$, tiene ventaja

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

Comentario 19 *Una permutación π con $\mathcal{D}=\{0,1\}^d$ permuta cadenas en $\mathcal{D}$, no bits en una cadena. Por ejemplo, dado $d=3$, $\pi(k,010)$ podría ser 111, aunque estas cadenas tengan diferentes números de bits $=1$.*

Comentario 20 *Por motivos históricos y prácticos, los algoritmos de cifrado de bloque, o PRP, son entre los componentes mas usados (correctamente y no) y estudiados de la criptología. Hoy en día, el mas utilizado es el Advanced Encryption Standard (AES), que tolera $\mathcal{D}=\{0,1\}^{128}$ y presenta tres variantes: AES-128, con $|k|=128$, AES-192, con $|k|=192$, AES-256, con $|k|=256$. Se estima que AES-λ ofrece $\lambda=\log_2(t/\varepsilon)$ bits de seguridad (ε,t,q)-PRP.*



Los algoritmos de cifrado de bloque se utilizan a menudo en "modos de operacion". Pueden haber oído de ECB-mode (un modo prácticamente siempre inseguro), CBC-, CTR-, GCM-... No vamos a estudiar todos estos, dados que a menudo pensar en términos de modos de operación, en lugar que en términos de modelos de seguridad, puede resultar en la introducción de vulnerabilidades en protocolos. En efecto, vamos a cubrir métodos equivalentes al CTR y GCM.
PRGs, PRFs y PRPs son equivalentes, o sea:

- PRP $\Rightarrow$ PRF: "PRP-PRF switching lemma"
- PRF $\Rightarrow$ PRP: "Feistel networks"
- PRF $\Rightarrow$ PRG: $F(k,x_1)||\cdots||F(k,x_q)$
- PRG $\Rightarrow$ PRF: "GGM"

En el resto del curso, usaremos este postulado.

Postulado 2 *Dados (ε,t,q), las (ε,t,q)-PRP existen.*

Completamos este tema, construyendo PRFs de PRPs, y PRGs de PRFs.

3.1 De PRP a PRF

La idea de esta construcción es que una PRP es una PRF, si $\mathcal{A}$ observa pocos outputs. Para demostrarlo, primero vemos dos lemas requeridos.

Lemma 5 (Difference lemma, lema de la diferencia) *Sean E_1, E_2, Z tres eventos donde*

$$E_1 \wedge \overline{Z} \iff E_2 \wedge \overline{Z}.$$

Entonces $|\Pr[E_1] - \Pr[E_2]| \leq \Pr[Z]$.

Comentario 21 *"Si se necesita Z para distinguir E_1 de E_2, la probabilidad de distinguirlos es al máximo la probabilidad de que Z suceda."*

Demostración. Calculamos

$$\begin{aligned} |\Pr[E_1] - \Pr[E_2]| &= \left|(\Pr[E_1 \wedge Z] + \cancel{\Pr[E_1 \wedge \overline{Z}]}) - (\cancel{\Pr[E_2 \wedge Z]} + \Pr[E_2 \wedge \overline{Z}])\right| \\ &= |\Pr[E_1 \wedge Z] - \Pr[E_2 \wedge Z]|. \end{aligned}$$

Dado que $0 \leq \Pr[E_i \wedge Z] \leq \Pr[Z]$, con $i = 1, 2$,

$$\implies |\Pr[E_1 \wedge Z] - \Pr[E_2 \wedge Z]| \leq \Pr[Z].$$

□

Lemma 6 (Birthday bound, paradoja del cumpleaños) *Dados $q \in \mathbb{Z}_{>0}$, $\mathcal{R}$ un conjunto finito, y $z_1, \ldots, z_q \in \mathcal{R}$ muestreados $z_i \sim U(\mathcal{R})$ de manera independiente,*

$$\Pr[\exists i \neq j : z_i = z_j] \leq \frac{q(q-1)}{2|\mathcal{R}|}$$

Demostración. Calculamos

$$\begin{aligned} \Pr[\exists i \neq j : z_i = z_j] &= \Pr\left[\bigvee_{i \neq j} z_i = z_j\right] \\ &\leq \sum_{i \neq j} \Pr[z_i = z_j] && \text{(por la cota de la unión)} \\ &= \sum_{i \neq j} \frac{1}{|R|} = \binom{q}{2} \frac{1}{|R|} = \frac{q(q-1)}{2|\mathcal{R}|}. \end{aligned}$$

□

Comentario 22 *El birthday bound es una cota superior "tight" o "ajustada", o sea que el valor efectivo de la probabilidad de colisión es muy cercano a la cota. Efectivamente, también se puede demostrar una cota inferior muy cercana, de $\approx \frac{q(q-1)}{4|\mathcal{R}|}$ [KL20, Lemma A.15].*

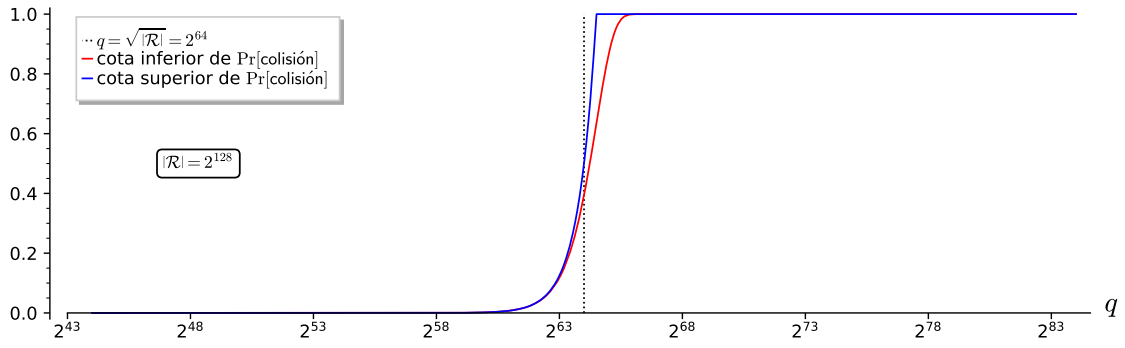


Figure 3: Visualizando las cotas en función de q, vemos que la probabilidad "salta" de ≈ 0 a ≈ 1 alrededor de $q = \sqrt{|R|}$.