

Clase 9: seguridad del cifrado “modo counter”

Fernando Virdia, versión: 0.1, mayo 2025

Teorema 5. Sean F, Π como en Definition 17. Si F es una (ε, t, q) -PRF, Π es (ε', t', q') -IND-CPA con $t' \approx t$, $q' = q/\ell$, $\varepsilon' = 2 \cdot \varepsilon + 2 \cdot q^2 \cdot \ell/|\mathcal{D}|$.

Proof. Dado un adversario $\mathcal{A}$ que juega Exp^{CPA} , definimos $\mathcal{B}$ que juega Exp^{PRF} teniendo acceso a un oráculo $\mathcal{O}$ definido como en Definition 13,

$\mathcal{B}^{\mathcal{O}(\cdot)}$	$E(m_0, m_1)$	$\widetilde{\text{Enc}}^{\mathcal{O}}(m)$
1: $\hat{b} \xleftarrow{\$} \{0, 1\}$	1: $c \leftarrow \widetilde{\text{Enc}}^{\mathcal{O}}(m_{\hat{b}})$	Lo mismo de Enc en Definition 17,
2: $\hat{b}' \leftarrow \mathcal{A}^E()$	2: return c	pero reemplazando $F(k, \cdot)$ con $\mathcal{O}(\cdot)$
3: return $[\hat{b}' = \hat{b}]$		

Notamos que el entorno de $\mathcal{A}$ en $\text{Exp}^{\text{PRF}}(\mathcal{B}, 0)$ es idéntico a la variante “bit-guessing” $\widetilde{\text{Exp}}^{\text{CPA}}(\mathcal{A})$. Sigue que

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

Lamentablemente, no es claro como calcular $\Pr[\text{Exp}^{\text{PRF}}(\mathcal{B}, 1) \Rightarrow 1]$ directamente. Por lo tanto, definimos un nuevo experimento $\widetilde{\text{Exp}}(\mathcal{B})$, idéntico a $\text{Exp}^{\text{PRF}}(\mathcal{B}, 1)$ pero donde reemplazamos el oráculo $\mathcal{O}$ que le viene dado a $\mathcal{B}$:

- En $\text{Exp}^{\text{PRF}}(\mathcal{B}, 1)$, $\forall x \mathcal{O}(x) := R(x)$, donde R es una función muestreada aleatoriamente.
- En $\widetilde{\text{Exp}}(\mathcal{B})$, reemplazamos $\mathcal{O}(x)$ con un **algoritmo** aleatorio $\hat{R}(x) = \text{“return } \$ \xleftarrow{\$} \{0, 1\}^r \text{”}$ que retorna elementos muestreados de $U(\{0, 1\}^r)$, ignorando el valor x en input. Esto quiere decir que mientras $\Pr[R(x) \neq R(x)] = 0$, $\Pr[\hat{R}(x) \neq \hat{R}(x)] = 1 - 2^{-r}$, en cuanto $\hat{R}$ **no es una función**.

Sea $G := \left| \Pr[\text{Exp}^{\text{PRF}}(\mathcal{B}, 1) \Rightarrow 1] - \Pr[\widetilde{\text{Exp}}(\mathcal{B}) \Rightarrow 1] \right|$. Definir $\widetilde{\text{Exp}}$ nos permite calcular,

$$\begin{aligned}
 \Pr[\widetilde{\text{Exp}}^{\text{CPA}}(\mathcal{A}) \Rightarrow 1] &= \left| \Pr[\text{Exp}^{\text{PRF}}(\mathcal{B}, 0) \Rightarrow 1] \right| \\
 &= \left| \Pr[\text{Exp}^{\text{PRF}}(\mathcal{B}, 0) \Rightarrow 1] - \underbrace{\Pr[\text{Exp}^{\text{PRF}}(\mathcal{B}, 1) \Rightarrow 1] + \Pr[\text{Exp}^{\text{PRF}}(\mathcal{B}, 1) \Rightarrow 1]}_{=0} \right| \\
 &\leq \text{Adv}(\text{Exp}^{\text{PRF}}, \mathcal{B}) + \left| \Pr[\text{Exp}^{\text{PRF}}(\mathcal{B}, 1) \Rightarrow 1] - \underbrace{\Pr[\widetilde{\text{Exp}}(\mathcal{B}) \Rightarrow 1] + \Pr[\widetilde{\text{Exp}}(\mathcal{B}) \Rightarrow 1]}_{=0} \right| \\
 &\leq \text{Adv}(\text{Exp}^{\text{PRF}}, \mathcal{B}) + G + \Pr[\widetilde{\text{Exp}}(\mathcal{B}) \Rightarrow 1]
 \end{aligned}$$

Empezamos calculando $\Pr[\widetilde{\text{Exp}}(\mathcal{B}) \Rightarrow 1]$. La vista de $\mathcal{A}$ en $\widetilde{\text{Exp}}(\mathcal{B})$ es tal que la i -ésima query a E retorna

$$E(m_{0,i}, m_{1,i}) = (c_{0,i}, m_{\hat{b},i,1} \oplus \hat{R}(z_{i,1}), \dots, m_{\hat{b},i,j} \oplus \hat{R}(z_{i,j}), \dots, m_{\hat{b},i,\ell} \oplus \hat{R}(z_{i,\ell}))$$

donde $z_{i,j} = c_{0,i} + j - 1 \bmod 2^d$, y donde $\hat{R}(z_{i,j}) \sim_{\text{iid}} U(\{0, 1\}^r)$. En particular, esta vista es independiente de $\hat{b}$ dado que cada bit de $E(m_{0,i}, m_{1,i})$ esta uniformemente distribuido por definicion de $c_{0,i}$ y de $\hat{R}$,

$$\begin{aligned}
 \Pr[m_{0,i,j} \oplus \hat{R}(z_{i,j}) = c_{j,i}] &= \Pr[\hat{R}(z_{i,j}) = c_{j,i} \oplus m_{0,i,j}] \\
 &= 2^{-r} \\
 &= \Pr[\hat{R}(z_{i,j}) = c_{j,i} \oplus m_{1,i,j}] \\
 &= \Pr[m_{1,i,j} \oplus \hat{R}(z_{i,j}) = c_{j,i}].
 \end{aligned}$$

Siendo la vista de $\mathcal{A}$ completamente independiente de $\hat{b}$ en $\widetilde{\text{Exp}}(\mathcal{B})$, así tambien lo es la salida $\hat{b}' \leftarrow \mathcal{A}^E()$, por lo que

$$\Pr[\hat{b}' = \hat{b}] = \Pr[\widetilde{\text{Exp}}(\mathcal{B}) \Rightarrow 1] = \frac{1}{2},$$

y de consecuencia

$$\text{Adv}(\overline{\text{Exp}}^{\text{CPA}}, \mathcal{A}) = \left| \Pr[\overline{\text{Exp}}^{\text{CPA}}(\mathcal{A}) \Rightarrow 1] - \frac{1}{2} \right| \leq \text{Adv}(\text{Exp}^{\text{PRF}}, \mathcal{B}) + G.$$

Nos queda calcular G , la ventaja de distinguir $\text{Exp}^{\text{PRF}}(\mathcal{B}, 1)$ de $\widetilde{\text{Exp}}(\mathcal{B})$. Notamos que la sola diferencia entre estos juegos es que $R(\cdot)$ es una función dentro de $\text{Exp}^{\text{PRF}}(\mathcal{B}, 1)$, por lo que $R(x)$ es un valor fijo, y $\hat{R}$ dentro de $\widetilde{\text{Exp}}(\mathcal{B})$ muestra uniformemente de $\{0, 1\}^r$, por lo que $\hat{R}(x)$ no tiene un valor fijo. Esta diferencia puede solo ser notada si $\mathcal{O}(\cdot)$ viene llamado sobre un mismo input $z_{i,j}$ mas de una vez durante el experimento. Sea

$$Z := “\exists i, i' \in [q], j, j' \in [\ell] : (i, j) \neq (i', j') \wedge z_{i,j} = z_{i',j'}, \text{ en } \text{Exp}^{\text{PRF}}(\mathcal{B}, 1)”$$

el evento por el cual $\mathcal{O}(\cdot)$ viene llamado sobre un input $z_{i,j} = z_{i',j'}$ repetido durante el experimento $\text{Exp}^{\text{PRF}}(\mathcal{B}, 1)$. Notamos que $\text{Exp}^{\text{PRF}}(\mathcal{B}, 1)$ y $\widetilde{\text{Exp}}(\mathcal{B})$ son idénticos si Z no ocurre. Por lo tanto, usando el lema de la diferencia,

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

Sea

$$\text{coll}_{i,i'} := “\exists j, j' \in [\ell] : (i, j) \neq (i', j') \wedge z_{i,j} = z_{i',j'} \text{ en } \text{Exp}^{\text{PRF}}(\mathcal{B}, 1)”.$$

Por suposición, $\ell \leq 2^d/2$ (c.f. Definition 17). Esto quiere decir que

$$\Pr[\text{coll}_{i,i'} \mid i' = i] = 0,$$

dado que

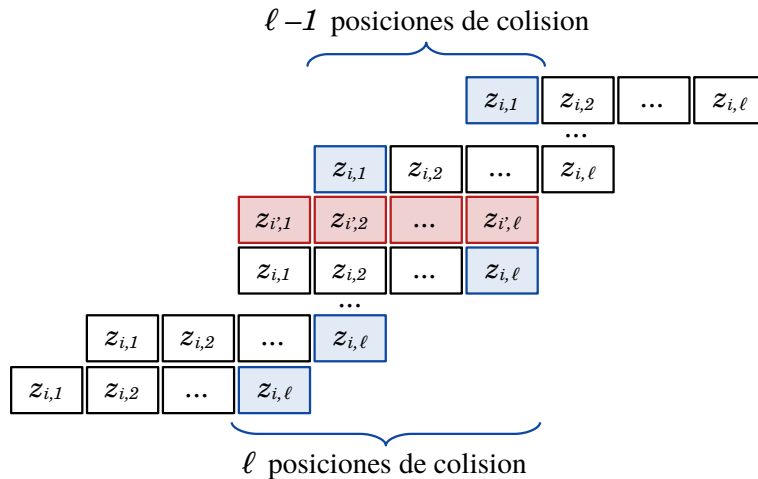
$$\begin{aligned} z_{i,j} = z_{i,j'} \wedge j \neq j' &\iff c_{0,i} + j - 1 = c_{0,i} + j' - 1 \bmod 2^d \wedge j \neq j' \\ &\iff j = j' \bmod 2^d \wedge j \neq j' \\ &\iff j = j' + \Delta 2^d \text{ donde } \Delta \in \mathbb{Z} \setminus \{0\} \\ &\iff \text{la } i\text{-ésima query es } \ell \geq 2^d \text{ bloques larga,} \end{aligned}$$

pero $\ell \leq 2^d/2$. Por lo tanto

$$\Pr[\text{coll}_{i,i'}] = \Pr[\text{coll}_{i,i'} \mid i = i'] \Pr[i = i'] + \Pr[\text{coll}_{i,i'} \mid i \neq i'] \Pr[i \neq i'] \leq \Pr[\text{coll}_{i,i'} \mid i \neq i'].$$

Supongamos entonces que $i \neq i'$. Queremos calcular la probabilidad de una colisión entre

$$(z_{i,1}, \dots, z_{i,\ell}) \quad \text{y} \quad (z_{i',1}, \dots, z_{i',\ell}).$$



Para que haya una colisión, $z_{i,1}$ tiene que tener un valor que sobreponga las dos secuencias. Solo hay $2 \cdot \ell - 1$ tales valores posibles de $z_{i,1} = c_{0,i}$ para que suceda una colisión, donde $c_{0,i}$ es muestrado aleatoriamente en $\widetilde{\text{Enc}}$. Esto implica que $\Pr[\text{coll}_{i,i'} \mid i \neq i'] = \frac{2 \cdot \ell - 1}{2^d}$. Finalmente, podemos calcular

$$\Pr[Z] = \Pr \left[\bigvee_{i \neq i'} \text{coll}_{i,i'} \right] \leq \sum_{i \neq i'} \Pr[\text{coll}_{i,i'}] \leq \binom{q}{2} \frac{2 \cdot \ell - 1}{2^d} \leq \frac{q \cdot (q - 1)}{2} \cdot \frac{2 \cdot \ell}{2^d} \leq \frac{q^2 \cdot \ell}{2^d}$$

Con esto, podemos completar el calculo de la ventaja de $\mathcal{A}$, recordando que

$$\text{Adv}(\text{Exp}^{\text{CPA}}, \mathcal{A}) = 2 \cdot \text{Adv}(\overline{\text{Exp}^{\text{CPA}}}, \mathcal{A}) \leq 2 \cdot \left(\text{Adv}(\text{Exp}^{\text{PRF}}, \mathcal{B}) + \Pr[Z] \right) \leq 2 \cdot \left(\text{Adv}(\text{Exp}^{\text{PRF}}, \mathcal{B}) + \frac{q^2 \cdot \ell}{2^d} \right),$$

lo que nos da $t' \approx t$, $q' = q/\ell$, y $\varepsilon' = 2 \cdot \varepsilon + \frac{2 \cdot q^2 \cdot \ell}{2^d}$, donde $|\mathcal{D}| = 2^d$. $\square$

Comentario 32. Nuevamente vemos una diferencia en ventaja relacionada a una probabilidad de colisión. Este tipo de ataque es verosímil, como en el caso del ataque <https://sweet32.info>.

Finalmente podemos cifrar múltiples mensajes de ℓ “bloques” de r bits de largo. Si un mensaje es $> \ell$ bloques, se lo puede transmitir como dos mensajes. Formalmente, se lo puede demostrar como un lema.

Lemma 9 (fixed-length IND-CPA $\Rightarrow$ variable-length IND-CPA). Sea $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ un SKES que otorga seguridad (ε, t, q) -IND-CPA. Sea $\Pi' = (\text{Gen}', \text{Enc}', \text{Dec}')$ un SKES con

- $\text{Gen}' = \text{Gen}$,
- $\text{Enc}'(k, (m_1, m_2)) := (\text{Enc}(k, m_1), \text{Enc}(k, m_2))$,
- $\text{Dec}(k, (c_1, c_2)) := (\text{Dec}(k, c_1), \text{Dec}(k, c_2))$.

Π' es (ε', t', q') -IND-CPA donde $\varepsilon' = \dots$, $t' \approx \dots$, $q' = \dots$.

EJERCICIO: Determina (ε', t', q') .

EJERCICIO: El Lemma 9 dice que podemos utilizar multiples cifrados IND-CPA para obtener fixed-length IND-CPA. El OTP es OT-IND-CPA, pero no puede ser re-utilizado. Por que esta no es una contradicción?