Clase 9: seguridad del cifrado "modo counter"

Fernando Virdia, versión: 0.0.1, junio 2024

Teorema 5 *Sean F, Π como en Definition 13. Si F es una (ε, t, q)-PRF, Π es (ε', t', q')-IND-CPA con $t' \approx t$, $q' = q/\ell$, $\varepsilon' = 2 \cdot \varepsilon + 2 \cdot q^2 \cdot \ell / |\mathcal{D}|$.*

Demostración. Dado un adversario $\mathcal{A}$ que juega $\mathsf{Exp}^{\mathrm{CPA}}$, definimos $\mathcal{B}$ que juega $\mathsf{Exp}^{\mathrm{PRF}}$,

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

Notamos que el entorno de $\mathcal{A}$ en $\mathsf{Exp}^{\mathrm{PRF}}(\mathcal{B}, 0)$ es idéntico a la variante "bit-guessing" $\overline{\mathsf{Exp}^{\mathrm{CPA}}}(\mathcal{A})$. Sigue que

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

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

- En $\mathsf{Exp}^{\mathrm{PRF}}(\mathcal{B}, 1)$, $\mathcal{O}(\cdot) = R(\cdot)$, una función muestreada aleatoriamente.
- En $\widetilde{\mathsf{Exp}}(\mathcal{B})$, remplazamos $\mathcal{O}(\cdot)$ con un **algoritmo** aleatorio $\hat{R}(x) =$ "**return** $\$ \xleftarrow{\$} \{0,1\}^r$" 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 $G \coloneqq \left|\Pr[\mathsf{Exp}^{\mathrm{PRF}}(\mathcal{B}, 1) \Rightarrow 1] - \Pr[\widetilde{\mathsf{Exp}}(\mathcal{B}) \Rightarrow 1]\right|$. Definir $\widetilde{\mathsf{Exp}}$ nos permite calcular,

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

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

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

donde $z_{i,j} = c_{0,i} + j - 1 \bmod 2^d$, y donde $\hat{R}(z_{i,j}) \sim_{\mathrm{iid}} U(\{0,1\}^r)$. En particular, esta vista es independiente de $\hat{b}$ dado que

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

Al ser la salida $\hat{b}' \leftarrow \mathcal{A}^{E}()$ independiente de $\hat{b} \xleftarrow{\$} \{0,1\}$,

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

y de consecuencia

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

Nos queda calcular G, la ventaja de distinguir $\mathsf{Exp}^{\mathrm{PRF}}(\mathcal{B}, 1)$ de $\widetilde{\mathsf{Exp}}(\mathcal{A})$. Notamos que la sola diferencia entre estos juegos es que $R(\cdot)$ es una función, por lo que $R(x)$ es un valor fijo, y $\hat{R}$ no. 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 $Z :=$ "$\exists (i,j) \neq (i',j') : z_{i,j} = z_{i',j'}$" el evento por el cual $\mathcal{O}(\cdot)$ viene llamado sobre un input repetido durante el experimento. Notamos que $\mathsf{Exp}^{\mathrm{PRF}}(\mathcal{B}, 1)$ y $\widetilde{\mathsf{Exp}}(\mathcal{A})$ son idénticos si Z no ocurre. Por lo tanto, usando el *lema de la diferencia*,

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

Sea $\mathsf{coll}_{i,i'}$ el evento "hay una colisión entre $\{z_{i,1}, \ldots, z_{i,\ell}\}$ y $\{z_{i',1}, \ldots, z_{i',\ell}\}$". En particular, sea esta $z_{i,j} = z_{i',j'}$.

Por suposición, $\ell \leq 2^d/2$. Esto quiere decir que

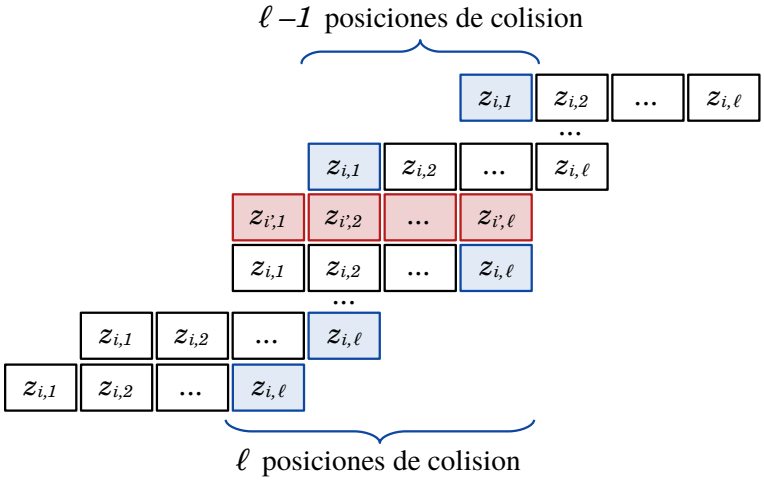
$$\Pr[\mathsf{coll}_{i,i'} \mid i' = i] = 0,$$

dado que no puede haber una colisión en $\{z_{i,j} = c_{0,i} + j - 1 \bmod 2^d\}_{j=1}^{\ell}$ en cuanto ℓ elementos no son suficientes para circular modulo 2^d y colisionar. Por lo tanto

$$\Pr[\mathsf{coll}_{i,i'}] = \cancelto{0}{\Pr[\mathsf{coll}_{i,i'} \mid i = i']} \Pr[i = i'] + \Pr[\mathsf{coll}_{i,i'} \mid i \neq i'] \Pr[i \neq i'] \leq \Pr[\mathsf{coll}_{i,i'} \mid i \neq i'].$$

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

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



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, lo que implica que $\Pr[\mathsf{coll}_{i,i'} \mid i \neq i'] = \frac{2 \cdot \ell - 1}{2^d}$. Finalmente, podemos calcular

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

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

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

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

Comentario 29 *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* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *un SKES que otorga seguridad* (ε, t, q)*-IND-CPA. Sea* $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ *un SKES con*

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

Π' *es* (ε', t', q')*-IND-CPA.*
EJERCICIO: *Determina* (ε, t, q).