

# Clase 16: cifrado de clave publica multi-mensaje

Fernando Virdia, versión: 0.1, mayo 2025

**Definición 34** (IND-CPA). Sea  $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$  un PKES.

| $\text{Exp}^{\text{CPA}}(\mathcal{A}, b)$               | $\mathcal{O}(m_0, m_1)$                      |
|---------------------------------------------------------|----------------------------------------------|
| 1: $(\text{sk}, \text{pk}) \leftarrow \text{Gen}()$     | 1: $c \leftarrow \text{Enc}(\text{pk}, m_b)$ |
| 2: $b' \leftarrow \mathcal{A}^{\mathcal{O}}(\text{pk})$ | 2: <b>return</b> $c$                         |
| 3: <b>return</b> $b'$                                   |                                              |

Decimos que  $\Pi$  otorga  $(\varepsilon, t, q)$ -indistinguibilidad bajo ataques de mensaje elegido (IND-CPA, “indistinguishability under chosen-plaintext attacks”), si cualquier adversario  $\mathcal{A}$  que corre en tiempo  $\leq t$  y usa  $\leq q$  queries a  $\mathcal{O}$ , tiene ventaja

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

**Comentario 54.** Respecto a la definición simétrica, no escribimos explícitamente el requisito  $|m_1| = |m_2|$  simplemente por que generalmente  $m_i \notin \{0, 1\}^*$ , y tienen un tamaño predeterminado.

**Lemma 17** (PKE OT-IND-CPA  $\Rightarrow$  PKE IND-CPA). Sea  $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$  un PKES que ofrece  $(\varepsilon, t)$ -OT-IND-CPA. Entonces ofrece  $(\varepsilon', t', q)$ -IND-CPA con  $\varepsilon' = q \cdot \varepsilon$ ,  $t' \approx t$ .

*Proof.* Supongamos un adversario  $\mathcal{A}$  que usa  $q$  queries contra  $\text{Exp}^{\text{CPA}}$ . Definimos  $q$  adversarios  $\mathcal{B}_1, \dots, \mathcal{B}_q$  contra  $\text{Exp}^{\text{OT-CPA}}$ .

| $\mathcal{B}_i^E(\text{pk})$                            | $\mathcal{O}(m_0, m_1)$                      |
|---------------------------------------------------------|----------------------------------------------|
| 1: $\text{cnt} \leftarrow 0$                            | 1: $\text{cnt} \leftarrow \text{cnt} + 1$    |
| 2: $b' \leftarrow \mathcal{A}^{\mathcal{O}}(\text{pk})$ | 2: <b>if</b> $\text{cnt} < i$ :              |
| 3: <b>return</b> $b'$                                   | 3: $c \leftarrow \text{Enc}(\text{pk}, m_0)$ |
|                                                         | 4: <b>elseif</b> $\text{cnt} = i$ :          |
|                                                         | 5: $c \leftarrow E(m_0, m_1)$                |
|                                                         | 6: <b>else</b> :                             |
|                                                         | 7: $c \leftarrow \text{Enc}(\text{pk}, m_1)$ |
|                                                         | 8: <b>return</b> $c$                         |

Notemos que siendo  $\Pi$   $(\varepsilon, t)$ -OT-IND-CPA,

$$\left| \Pr[\text{Exp}^{\text{OT-CPA}}(\mathcal{B}_i, 0) \Rightarrow 1] - \Pr[\text{Exp}^{\text{OT-CPA}}(\mathcal{B}_i, 1) \Rightarrow 1] \right| \leq \varepsilon \quad \forall i \in [q].$$

Inspeccionemos el patrón de como los  $\mathcal{B}_i$  les responden queries a  $\mathcal{A}$  dentro de  $\text{Exp}^{\text{OT-CPA}}(\mathcal{B}_i, b)$ . En lo siguiente escribimos  $\mathcal{E}(m)$  en lugar de  $\text{Enc}(\text{pk}, m)$ .

| adversario          | $b$ | numero de query    |     |                    |                    |                    |     |                    |
|---------------------|-----|--------------------|-----|--------------------|--------------------|--------------------|-----|--------------------|
|                     |     | 1                  | ... | $i-1$              | $i$                | $i+1$              | ... | $q$                |
| $\mathcal{B}_1$     | 1   | $\mathcal{E}(m_1)$ | ... | $\mathcal{E}(m_1)$ | $\mathcal{E}(m_1)$ | $\mathcal{E}(m_1)$ | ... | $\mathcal{E}(m_1)$ |
| $\mathcal{B}_1$     | 0   | $\mathcal{E}(m_0)$ | ... | $\mathcal{E}(m_1)$ | $\mathcal{E}(m_1)$ | $\mathcal{E}(m_1)$ | ... | $\mathcal{E}(m_1)$ |
| $\vdots$            |     |                    |     |                    |                    |                    |     |                    |
| $\mathcal{B}_{i-1}$ | 1   | $\mathcal{E}(m_0)$ | ... | $\mathcal{E}(m_1)$ | $\mathcal{E}(m_1)$ | $\mathcal{E}(m_1)$ | ... | $\mathcal{E}(m_1)$ |
| $\mathcal{B}_{i-1}$ | 0   | $\mathcal{E}(m_0)$ | ... | $\mathcal{E}(m_0)$ | $\mathcal{E}(m_1)$ | $\mathcal{E}(m_1)$ | ... | $\mathcal{E}(m_1)$ |
| $\mathcal{B}_i$     | 1   | $\mathcal{E}(m_0)$ | ... | $\mathcal{E}(m_0)$ | $\mathcal{E}(m_1)$ | $\mathcal{E}(m_1)$ | ... | $\mathcal{E}(m_1)$ |
| $\mathcal{B}_i$     | 0   | $\mathcal{E}(m_0)$ | ... | $\mathcal{E}(m_0)$ | $\mathcal{E}(m_0)$ | $\mathcal{E}(m_1)$ | ... | $\mathcal{E}(m_1)$ |
| $\mathcal{B}_{i+1}$ | 1   | $\mathcal{E}(m_0)$ | ... | $\mathcal{E}(m_0)$ | $\mathcal{E}(m_0)$ | $\mathcal{E}(m_1)$ | ... | $\mathcal{E}(m_1)$ |
| $\vdots$            |     |                    |     |                    |                    |                    |     |                    |
| $\mathcal{B}_q$     | 0   | $\mathcal{E}(m_0)$ | ... | $\mathcal{E}(m_0)$ | $\mathcal{E}(m_0)$ | $\mathcal{E}(m_0)$ | ... | $\mathcal{E}(m_0)$ |

Notamos el siguiente patrón:

$$\forall i < q, \quad \Pr[\text{Exp}^{\text{OT-CPA}}(\mathcal{B}_i, 0) \Rightarrow 1] = \Pr[\text{Exp}^{\text{OT-CPA}}(\mathcal{B}_{i+1}, 1) \Rightarrow 1]. \quad (\star)$$

también notamos que del punto de vista de  $\mathcal{A}$ ,  $\text{Exp}^{\text{CPA}}(\mathcal{A}, 1)$  es idéntico a  $\text{Exp}^{\text{OT-CPA}}(\mathcal{B}_1, 1)$ , y  $\text{Exp}^{\text{CPA}}(\mathcal{A}, 0)$  es idéntico a  $\text{Exp}^{\text{OT-CPA}}(\mathcal{B}_q, 0)$ . Por lo tanto,

$$\begin{aligned} \text{Adv}(\text{Exp}^{\text{CPA}}, \mathcal{A}) &= \left| \Pr[\text{Exp}^{\text{CPA}}(\mathcal{A}, 0) \Rightarrow 1] - \Pr[\text{Exp}^{\text{CPA}}(\mathcal{A}, 1) \Rightarrow 1] \right| \\ &= \left| \Pr[\text{Exp}^{\text{OT-CPA}}(\mathcal{B}_q, 0) \Rightarrow 1] - \Pr[\text{Exp}^{\text{OT-CPA}}(\mathcal{B}_1, 1) \Rightarrow 1] \right| \\ &= \left| \Pr[\text{Exp}^{\text{OT-CPA}}(\mathcal{B}_q, 0) \Rightarrow 1] \right. \\ &\quad \left. - \underbrace{\Pr[\text{Exp}^{\text{OT-CPA}}(\mathcal{B}_q, 1) \Rightarrow 1] + \Pr[\text{Exp}^{\text{OT-CPA}}(\mathcal{B}_{q-1}, 0) \Rightarrow 1]}_{= 0 \text{ por } (\star)} \right. \\ &\quad \left. - \Pr[\text{Exp}^{\text{OT-CPA}}(\mathcal{B}_1, 1) \Rightarrow 1] \right| \\ &\leq \text{Adv}(\text{Exp}^{\text{OT-CPA}}, \mathcal{B}_q) + \left| \Pr[\text{Exp}^{\text{OT-CPA}}(\mathcal{B}_{q-1}, 0) \Rightarrow 1] - \Pr[\text{Exp}^{\text{OT-CPA}}(\mathcal{B}_1, 1) \Rightarrow 1] \right| \\ &\leq \text{Adv}(\text{Exp}^{\text{OT-CPA}}, \mathcal{B}_q) + \left| \Pr[\text{Exp}^{\text{OT-CPA}}(\mathcal{B}_{q-1}, 0) \Rightarrow 1] \right. \\ &\quad \left. - \underbrace{\Pr[\text{Exp}^{\text{OT-CPA}}(\mathcal{B}_{q-1}, 1) \Rightarrow 1] + \Pr[\text{Exp}^{\text{OT-CPA}}(\mathcal{B}_{q-2}, 0) \Rightarrow 1]}_{= 0 \text{ por } (\star)} \right. \\ &\quad \left. - \Pr[\text{Exp}^{\text{OT-CPA}}(\mathcal{B}_1, 1) \Rightarrow 1] \right| \\ &\leq \text{Adv}(\text{Exp}^{\text{OT-CPA}}, \mathcal{B}_q) + \text{Adv}(\text{Exp}^{\text{OT-CPA}}, \mathcal{B}_{q-1}) + \left| \Pr[\text{Exp}^{\text{OT-CPA}}(\mathcal{B}_{q-2}, 0) \Rightarrow 1] - \Pr[\text{Exp}^{\text{OT-CPA}}(\mathcal{B}_1, 1) \Rightarrow 1] \right| \\ &\quad \vdots \\ &\leq \sum_{k=q}^2 \text{Adv}(\text{Exp}^{\text{OT-CPA}}, \mathcal{B}_k) + \left| \Pr[\text{Exp}^{\text{OT-CPA}}(\mathcal{B}_1, 0) \Rightarrow 1] - \Pr[\text{Exp}^{\text{OT-CPA}}(\mathcal{B}_1, 1) \Rightarrow 1] \right| \\ &= \sum_{k=q}^1 \text{Adv}(\text{Exp}^{\text{OT-CPA}}, \mathcal{B}_k) \leq \sum_{k=q}^1 \varepsilon = q \cdot \varepsilon. \end{aligned}$$

Notamos que  $\mathcal{B}_i$  y  $\mathcal{A}$  corren en tiempo parecido, por lo que  $t' \approx t$ , y que si  $\mathcal{A}$  usa  $\leq q$  queries,  $\varepsilon' \leq q \cdot \varepsilon$ . Por lo tanto, si  $\Pi$  es  $(\varepsilon, t)$ -OT-IND-CPA, entonces también es  $(q \cdot \varepsilon, \approx t, q)$ -IND-CPA.  $\square$

**Comentario 55.** La técnica que acabamos de usar se llama argumento híbrido (“hybrid argument”), porque requiere definir experimentos “híbridos” entre  $\text{Exp}^{\text{CPA}}(\mathcal{A}, 0)$  y  $\text{Exp}^{\text{CPA}}(\mathcal{A}, 1)$  con los cuales calculamos la ventaja total, utilizando la ventaja de distinguir pares de híbridos.

**Comentario 56.** Lemma 17 implica un modo de cifrar mensajes  $m \in \{0, 1\}^*$  arbitrariamente largos. Sea  $m = m_1, m_2, \dots, m_n$  una cadena de  $n$  bits. Podemos generar una cadena de cifrados

$$\text{Enc}'(\text{pk}, m \in \{0, 1\}^n) := (\text{Enc}(\text{pk}, g^{m_1}), \text{Enc}(\text{pk}, g^{m_2}), \dots, \text{Enc}(\text{pk}, g^{m_n}))$$

donde  $g^{m_i}$  es  $g^1$  si  $m_i = 1$  y  $g^0 = e$  si  $m_i = 0$ . Si  $\Pi$  es  $(\varepsilon, t, q)$ -IND-CPA con  $q \geq n$ , el cifrado es seguro. Notablemente, no solo esta técnica es muy ineficiente (vamos a ver una mejor alternativa), si no que también no funciona con nociones de seguridad mas fuertes, como IND-CCA.

**Comentario 57.** A diferencia de SKE (c.f. Remark 29), en el caso de PKE, OT-IND-CPA  $\implies$  IND-CPA.

**EJERCICIO:** Por que existe esta diferencia?

Por que en el caso de PKE, el adversario siempre puede evaluar  $\text{Enc}(\text{pk}, m)$  internamente. Esto le permite implementar  $\mathcal{E}(m)$  en la demostración.

En el caso SKE, para evaluar  $\text{Enc}(k, m)$  el adversario  $\mathcal{B}$  contra  $\text{Exp}^{\text{OT-CPA}}$  tiene que utilizar la sola query al oraculo de cifrado  $E(\cdot, \cdot)$  otorgadole por  $\text{Exp}^{\text{OT-CPA}}$  para realizar  $\mathcal{E}(m) = E(\cdot, \cdot)$  en el primer “hop”. Inmediatamente  $\mathcal{B}$  se quedaria sin acceso al oraculo, impidiendole completar la demostración.