Clase 16: cifrado de clave publica multi-mensaje

Fernando Virdia, versión: 0.0.1, junio 2024

Definición 30 (IND-CPA) *Sea* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *un PKES.*

$\mathsf{Exp}^{\text{CPA}}(\mathcal{A}, b)$	$\mathcal{O}(m_0, m_1)$
$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}()$	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m_b)$
$b' \leftarrow \mathcal{A}^{\mathcal{O}}(\mathsf{pk})$	**return** c
return b'	

Decimos que Π *otorga* (ε, t, q)*-indistinguibilidad bajo ataques de mensaje elegido (IND-CPA, "indistinguishibility 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*

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

Comentario 52 *Respecto a la definición simétrica, no escribimos explícitamente el requisito* $|m_1| = |m_2|$ *simplemente por que los conjuntos de mensaje sólidamente no son naturalmente* $\{0,1\}^*$*. De cualquier manera, el leak de información sobre* $m \in \mathcal{M}$ *a través de* c *queda presente.*

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

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

$\mathcal{B}_i^{E}(\mathsf{pk})$	$\mathcal{O}(m_0, m_1)$
$\mathsf{cnt} \leftarrow 0$	$\mathsf{cnt} \leftarrow \mathsf{cnt} + 1$
$b' \leftarrow \mathcal{A}^{\mathcal{O}}(\mathsf{pk})$	**if** $\mathsf{cnt} < i$:
return b'	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m_0)$
	elseif $\mathsf{cnt} = i$:
	$c \leftarrow E(m_0, m_1)$
	else :
	$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m_1)$
	return c

Notemos que siendo Π (ε, t)-OT-IND-CPA,

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

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

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

Notamos el siguiente patrón:

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

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

$$\begin{aligned}
\mathsf{Adv}(\mathsf{Exp}^{\text{CPA}}, \mathcal{A}) &= \left|\Pr[\mathsf{Exp}^{\text{CPA}}(\mathcal{A}, 0) \Rightarrow 1] - \Pr[\mathsf{Exp}^{\text{CPA}}(\mathcal{A}, 1) \Rightarrow 1]\right| \\
&= \left|\Pr[\mathsf{Exp}^{\text{OT-CPA}}(\mathcal{B}_q, 0) \Rightarrow 1] - \Pr[\mathsf{Exp}^{\text{OT-CPA}}(\mathcal{B}_1, 1) \Rightarrow 1]\right| \\
&= \left|\begin{array}{l}\Pr[\mathsf{Exp}^{\text{OT-CPA}}(\mathcal{B}_q, 0) \Rightarrow 1] \\ \qquad \underbrace{- \Pr[\mathsf{Exp}^{\text{OT-CPA}}(\mathcal{B}_q, 1) \Rightarrow 1] + \Pr[\mathsf{Exp}^{\text{OT-CPA}}(\mathcal{B}_{q-1}, 0) \Rightarrow 1]}_{= 0 \text{ por } (\star)} \\ \qquad\qquad - \Pr[\mathsf{Exp}^{\text{OT-CPA}}(\mathcal{B}_1, 1) \Rightarrow 1]\end{array}\right| \\
&\leq \mathsf{Adv}(\mathsf{Exp}^{\text{OT-CPA}}, \mathcal{B}_q) + \left|\Pr[\mathsf{Exp}^{\text{OT-CPA}}(\mathcal{B}_{q-1}, 0) \Rightarrow 1] - \Pr[\mathsf{Exp}^{\text{OT-CPA}}(\mathcal{B}_1, 1) \Rightarrow 1]\right| \\
&\leq \mathsf{Adv}(\mathsf{Exp}^{\text{OT-CPA}}, \mathcal{B}_q) + \left|\begin{array}{l}\Pr[\mathsf{Exp}^{\text{OT-CPA}}(\mathcal{B}_{q-1}, 0) \Rightarrow 1] \\ \qquad \underbrace{- \Pr[\mathsf{Exp}^{\text{OT-CPA}}(\mathcal{B}_{q-1}, 1) \Rightarrow 1] + \Pr[\mathsf{Exp}^{\text{OT-CPA}}(\mathcal{B}_{q-2}, 0) \Rightarrow 1]}_{= 0 \text{ por } (\star)} \\ \qquad\qquad - \Pr[\mathsf{Exp}^{\text{OT-CPA}}(\mathcal{B}_1, 1) \Rightarrow 1]\end{array}\right| \\
&\leq \mathsf{Adv}(\mathsf{Exp}^{\text{OT-CPA}}, \mathcal{B}_q) + \mathsf{Adv}(\mathsf{Exp}^{\text{OT-CPA}}, \mathcal{B}_{q-1}) + \left|\Pr[\mathsf{Exp}^{\text{OT-CPA}}(\mathcal{B}_{q-2}, 0) \Rightarrow 1] - \Pr[\mathsf{Exp}^{\text{OT-CPA}}(\mathcal{B}_1, 1) \Rightarrow 1]\right| \\
&\vdots \\
&\leq \sum_{k=q}^{2} \mathsf{Adv}(\mathsf{Exp}^{\text{OT-CPA}}, \mathcal{B}_k) + \left|\Pr[\mathsf{Exp}^{\text{OT-CPA}}(\mathcal{B}_1, 0) \Rightarrow 1] - \Pr[\mathsf{Exp}^{\text{OT-CPA}}(\mathcal{B}_1, 1) \Rightarrow 1]\right| \\
&= \sum_{k=q}^{1} \mathsf{Adv}(\mathsf{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 Π es (ε, t)-OT-IND-CPA, entonces también es $(q \cdot \varepsilon, \approx t, q)$-IND-CPA. □

Comentario 53 *La técnica que acabamos de usar se llama argumento híbrido ("hybrid argument"), porque requiere definir experimentos "ibridos" entre* $\mathsf{Exp}^{\text{CPA}}(\mathcal{A}, 0)$ *y* $\mathsf{Exp}^{\text{CPA}}(\mathcal{A}, 1)$ *con los cuales calculamos la ventaja total, utilizando la ventaja de distinguir pares de híbridos.*

Comentario 54 *Lemma 17 implica un modo de cifrar mensajes* $m \in \{0,1\}^*$ *arbitrariamente largos. Sea* $m = m_1, m_2, \ldots, m_n$ *una cadena de* n *bits. Podemos generar una cadena de cifrados*

$$\mathsf{Enc}'(\mathsf{pk}, m \in \{0,1\}^n) \coloneqq (\mathsf{Enc}(\mathsf{pk}, g^{m_1}),\ \mathsf{Enc}(\mathsf{pk}, g^{m_2}),\ \ldots,\ \mathsf{Enc}(\mathsf{pk}, g^{m_n}))$$

donde g^{m_i} *es* g^1 *si* $m_i = 1$ *y* $g^0 = e$ *si* $m_i = 0$. *Si* Π *es* (ε, 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.*