Clase 15: cifrado de clave publica "one-time"

Fernando Virdia, versión: 0.0.1, junio 2024

9 Cifrado de Clave Publica

Como en el caso simétrico, empezamos definiendo nociones de cifrado.

Definición 27 (PKES, cifrado asimétrico o de clave publica) *Sean $\mathcal{K}_p$, $\mathcal{K}_s$, $\mathcal{M}$, $\mathcal{C}$ conjuntos. Decimos que $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ forman un cifrado asimétrico o de clave publica (PKES, "public-key encryption scheme") con espacio de claves publicas $\mathcal{K}_p$, de claves privadas $\mathcal{K}_s$, de mensajes $\mathcal{M}$, y de cifrados $\mathcal{C}$, si*

- Gen *es un algoritmo aleatorio,* $\mathsf{Gen}\colon \emptyset \to \mathcal{K}_s \times \mathcal{K}_p$ *que retorna una tupla (*sk, pk*). Decimos que* sk *es una clave privada, o secreta, ("secret key") y que* pk *es una clave publica ("public key").*
- Enc *es un algoritmo (posiblemente aleatorio),* $\mathsf{Enc}\colon \mathcal{K}_p \times \mathcal{M} \to \mathcal{C}$.
- Dec *es un algoritmo determinista* $\mathsf{Dec}\colon \mathcal{K}_s \times \mathcal{C} \to \mathcal{M}$.

Decimos que Π es δ-correcto si

$$\Pr_{\substack{(\mathsf{sk},\mathsf{pk})\sim\mathsf{Gen}(),\\ \$\ en\ \mathsf{Enc}}}[\mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, m; \$)) \neq m] \leq \delta,$$

donde Gen, Enc *y* Dec *son "eficientes" (corren en tiempo $\approx \log_2(|m|)$).*

Comentario 48 *Al definir SKES, requerimos que fueran δ-correcto con $\delta = 0$. No es así con PKES, porque varias técnicas para construir PKE resulta en sistemas eficientes si $\delta \gtrsim 0$ pero menos eficientes con $\delta = 0$. En el curso vamos a ver solo sistemas con $\delta = 0$.*

Comentario 49 *En nuestra definición usamos conjuntos $\mathcal{M}$ y $\mathcal{C}$. En practica, es común que al generar claves, implícitamente fijemos $\mathcal{M}_{\mathsf{pk}} \subset \mathcal{M}$ y $\mathcal{C}_{\mathsf{pk}} \subset \mathcal{C}$ donde se encuentran los mensajes y cifrados.*

Comentario 50 *Diferentemente de SKE, a menudo $\mathcal{K}_s$, $\mathcal{K}_p$, $\mathcal{M}$, $\mathcal{C}$* ***no son*** *conjuntos de cadenas de bits.*

Muchas de las ideas desarrolladas para SKE pueden ser adaptadas a PKE. Una diferencia crucial es que $\mathcal{A}$ recibe pk, al ser una clave publica, y esto le permite cifrar mensajes sin requerir un oráculo.

Definición 28 (OT-IND-CPA) *Sea $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ un PKES.*

$\mathsf{Exp}^{\text{OT-CPA}}(\mathcal{A}, b)$	$\mathcal{O}(m_0, m_1)$
1 : $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}()$	1 : **if** $\mathsf{disabled} = 1$:
2 : $\mathsf{disabled} \leftarrow 0$	2 : **return** $\perp$
3 : $b' \leftarrow \mathcal{A}^{\mathcal{O}}(\mathsf{pk})$	3 : $\mathsf{disabled} \leftarrow 1$
4 : **return** b'	4 : $c^* \leftarrow \mathsf{Enc}(\mathsf{pk}, m_b)$
	5 : **return** c^*

Decimos que Π otorga one-time (ε, t)-indistinguibilidad bajo ataques de mensaje elegido (OT-IND-CPA, "one-time indistinguishibility under chosen-plaintext attacks"), si cualquier adversario $\mathcal{A}$ que corre en tiempo $\leq t$ tiene ventaja

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

Comentario 51 *Aunque esta definición le ofrece a $\mathcal{A}$ un solo cifrado para distinguir b, a menudo la preferimos a una definición que ofrezca $q \geq 1$ cifrados. Esto es porque demostrar* OT-CPA *es mas fácil, y porque OT-IND-CPA $\Rightarrow$ IND-CPA.*

Vamos ahora a definir el PKES de ElGamal. Puede ser visto como una versión no interactiva del KEX de Diffie-Hellman.

Definición 29 (ElGamal PKE) *Sea $\mathbb{G} = (G, \times)$ un grupo cíclico generado por g. Sean $\mathcal{K}_s = [|G|]$, $\mathcal{K}_{\mathsf{pk}} = \mathcal{M} = \mathcal{C} = G$.*

$\mathsf{Gen}()$	$\mathsf{Enc}(\mathsf{pk} = g^x, m)$	$\mathsf{Dec}(\mathsf{sk} = x, c = (c_0, c_1))$
$x \xleftarrow{\$} [|G|]$	$y \xleftarrow{\$} [|G|]$	$m' \leftarrow c1 \times c_0^{-x}$
$\mathsf{sk} \leftarrow x$	$c_0 \leftarrow g^y$	**return** m'
$\mathsf{pk} \leftarrow g^x$	$c_1 \leftarrow (g^x)^y \times m$	
return $(\mathsf{sk}, \mathsf{pk})$	$c \leftarrow (c_0, c_1)$	
	return c	

Observamos que Π es δ-correcto con $\delta = 0$, dado que

$$m' = c1 \times c_0^{-x} = \cancel{(g^x)^y} \times m \times \cancel{(g^y)^{-x}} = m \quad \forall x, y \in [|G|].$$

Lemma 16 (ElGamal PKE + (ε, t)-DDH $\Rightarrow$ OT-IND-CPA) *Sea $\mathbb{G} = \langle g \rangle$ un grupo cíclico tal que DDH es (ε, t)-difícil. Sea Π el PKES de ElGamal definido sobre $\mathbb{G}$ con generador g. Entonces Π otorga (ε', t')-OT-IND-CPA con $\varepsilon' = 2 \cdot \varepsilon$, $t' \approx t$.*

Demostración. Supongamos un adversario $\mathcal{A}$ contra $\mathsf{Exp}^{\text{OT-CPA}}$. Definimos un adversario $\mathcal{B}$ contra $\mathsf{Exp}^{\text{DDH}}$.

$\mathcal{B}(g^x, g^y, g^z)$	$\mathcal{O}(m_0, m_1)$
$\mathsf{disabled} \leftarrow 0$	**if** $\mathsf{disabled} = 1$:
$\hat{b} \xleftarrow{\$} \{0, 1\}$	**return** $\perp$
$\hat{b}' \leftarrow \mathcal{A}^{\mathcal{O}}(g^x)$	$\mathsf{disabled} \leftarrow 1$
if $\hat{b}' = \hat{b}$:	$c^* \leftarrow (g^y, g^z \cdot m_{\hat{b}})$
return 0 //"$z = x \cdot y$"	**return** c^*
else	
return 1 //"$z \sim U([|G|])$"	

Recordemos la versión "bit-guessing" de $\mathsf{Exp}^{\text{OT-CPA}}$:

$\overline{\mathsf{Exp}^{\text{OT-CPA}}}(\mathcal{A})$
$\hat{b} \xleftarrow{\$} \{0, 1\}$
$\hat{b}' \leftarrow \mathsf{Exp}^{\text{OT-CPA}}(\mathcal{A}, \hat{b})$
return $[\![\hat{b}' = \hat{b}]\!]$

Usando la misma demostración de Lemma 3, sabemos que

$$\mathsf{Adv}(\overline{\mathsf{Exp}^{\text{OT-CPA}}}, \mathcal{A}) := \left| \Pr[\overline{\mathsf{Exp}^{\text{OT-CPA}}}(\mathcal{A}) \Rightarrow 1] - \frac{1}{2} \right| = \frac{1}{2} \mathsf{Adv}(\mathsf{Exp}^{\text{OT-CPA}}, \mathcal{A}).$$

Por inspección, podemos ver que el entorno de $\mathcal{A}$ en $\mathsf{Exp}^{\text{DDH}}(\mathcal{B}, 0)$, es idéntico al de $\mathcal{A}$ en $\overline{\mathsf{Exp}^{\text{OT-CPA}}}(\mathcal{A})$ si $\mathsf{pk} = g^x$ y $c_0^* = g^y$. Por ende,

$$\begin{aligned}
&\Pr[\mathsf{Exp}^{\text{DDH}}(\mathcal{B}, 0) \Rightarrow 1] = \Pr[\overline{\mathsf{Exp}^{\text{OT-CPA}}}(\mathcal{A}) \Rightarrow 0] = 1 - \Pr[\overline{\mathsf{Exp}^{\text{OT-CPA}}}(\mathcal{A}) \Rightarrow 1] \\
\iff &\Pr[\mathsf{Exp}^{\text{DDH}}(\mathcal{B}, 0) \Rightarrow 1] - \frac{1}{2} = \frac{1}{2} - \Pr[\overline{\mathsf{Exp}^{\text{OT-CPA}}}(\mathcal{A}) \Rightarrow 1] \\
\iff &\mathsf{Adv}(\overline{\mathsf{Exp}^{\text{OT-CPA}}}, \mathcal{A}) = \left| \Pr[\overline{\mathsf{Exp}^{\text{OT-CPA}}}(\mathcal{A}) \Rightarrow 1] - \frac{1}{2} \right| = \left| \Pr[\mathsf{Exp}^{\text{DDH}}(\mathcal{B}, 0) \Rightarrow 1] - \frac{1}{2} \right|.
\end{aligned}$$

Dentro de $\mathsf{Exp}^{\text{DDH}}(\mathcal{B}, 1)$, $\mathcal{A}$ recibe $(g^x, g^y, g^z \cdot m_{\hat{b}})$, donde $g^z \sim U(\mathbb{G})$, independientemente de (g^x, g^y). Por lo tanto, la vista de $\mathcal{A}$ es independiente de $\hat{b}$, dado que

$$\Pr[h = g^z \cdot m_0] = \Pr[g^z = h \cdot m_0^{-1}] = \frac{1}{|\mathbb{G}|} = \Pr[g^z = h \cdot m_1^{-1}] = \Pr[h = g^z \cdot m_1]$$

Al ser el valor $\hat{b}'$ retornado por $\mathcal{A}$ independiente de $\hat{b}$, y al ser $\hat{b} \sim U(\{0,1\})$, sigue que

$$\Pr[\hat{b}' \neq \hat{b}] = \Pr[\mathsf{Exp}^{\text{DDH}}(\mathcal{B}, 1) \Rightarrow 1] = \frac{1}{2}.$$

Finalmente,

$$\begin{aligned}
\mathsf{Adv}(\mathsf{Exp}^{\text{OT-CPA}}, \mathcal{A}) &= 2 \cdot \mathsf{Adv}(\overline{\mathsf{Exp}^{\text{OT-CPA}}}, \mathcal{A}) \\
&= 2 \cdot \left| \Pr[\mathsf{Exp}^{\text{DDH}}(\mathcal{B}, 0) \Rightarrow 1] - \frac{1}{2} \right| \\
&= 2 \cdot \left| \Pr[\mathsf{Exp}^{\text{DDH}}(\mathcal{B}, 0) \Rightarrow 1] - \Pr[\mathsf{Exp}^{\text{DDH}}(\mathcal{B}, 1) \Rightarrow 1] \right| \\
&= 2 \cdot \mathsf{Adv}(\mathsf{Exp}^{\text{DDH}}, \mathcal{B}).
\end{aligned}$$

Claramente, $t' \approx t$, $\varepsilon' = 2 \cdot \varepsilon$, y Π ofrece $(2\varepsilon, \approx t)$-OT-IND-CPA. □