

Clase 17: PKE y adversarios activos

Fernando Virdia, versión: 0.1, mayo 2025

9.1 Adversarios activos contra PKE

Al estudiar cifrado simétrico seguro contra adversarios activos, introducimos la noción de seguridad INT-CTXT (Definition 21). Esta propone que un adversario no debería ser capaz de crear cifrados simétricos válidos de manera independiente, a menos utilizar un oráculo de cifrado. Intuitivamente, esto quiere decir que si el adversario modifica un cifrado c en tránsito, estas modificaciones van a ser detectadas por quien los recibe, que rechazará c .

Ejemplo 8. *Adversarios activos son una preocupación también en el caso de PKE. Por ejemplo, dado un cifrado ElGamal $c = (c_1, c_2) = (g^y, g^{xy} \cdot m)$ de un mensaje $m \in \mathbb{G}$, $\mathcal{A}$ puede elegir cualquier elemento $\Delta \in \mathbb{G}$, y generar $c' = (c_1, c_2 \cdot \Delta)$, que descifraría a $m' = m \cdot \Delta$.*

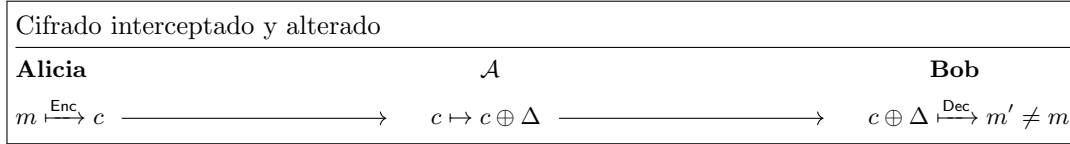
Lamentablemente, no es posible para un PKES otorgar seguridad INT-CTXT.

Ejemplo 9. *Sea $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ un PKES. Dada una clave pública pk , cualquier adversario $\mathcal{A}$ con acceso a pk puede evaluar $c \leftarrow \text{Enc}(\text{pk}, m)$ internamente, y obtener un cifrado c válido, sin requerir un oráculo de cifrado. Por lo tanto, una definición análoga a INT-CTXT no es inmediatamente traducible al caso PKE.*

Comentario 58. *En este ejemplo, aunque $\mathcal{A}$ ha generado cifrados válidos independientemente, estos no fueron obtenidos modificando cifrados en tránsito.*

Es posible obtener una definición de seguridad “intermedia” entre IND-CPA y AE que otorgue seguridad activa, aunque no otorgue INT-CTXT?

La respuesta es positiva, y pasa por capturar de qué manera un cifrado $c \oplus \Delta$ modificado por $\mathcal{A}$ puede resultar en un ataque.



En sí, $c \oplus \Delta$ no le da ninguna información a $\mathcal{A}$. Para serle útil, $\mathcal{A}$ tiene que mandarle $c \oplus \Delta$ a su víctima Bob, y observar como esta reacciona. De cierta manera, $\mathcal{A}$ necesita un *oráculo de descifrado* otorgado por Bob, que le permita observar la reacción de Bob al descifrar $c \oplus \Delta$.

Definición 35 (OT-IND-CCA PKE). *Sea $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ un PKES.*

Exp $\text{OT-IND-CCA}(\mathcal{A}, b)$	$\mathcal{O}(m_0, m_1)$	$D(c)$
1: $(\text{sk}, \text{pk}) \leftarrow \text{Gen}()$	1: if disabled = 1 :	1: if $c \in Q$:
2: disabled $\leftarrow 0$	2: return $\perp$	2: return $\perp$
3: $Q \leftarrow \{\}$	3: disabled $\leftarrow 1$	3: $m \leftarrow \text{Dec}(\text{sk}, c)$
4: $b' \leftarrow \mathcal{A}^{\mathcal{O}(\cdot), D(\cdot)}(\text{pk})$	4: $c \leftarrow \text{Enc}(\text{pk}, m_b)$	4: return m
5: return b'	5: $Q \leftarrow Q \cup \{c\}$	
	6: return c	

Decimos que Π otorga $(\varepsilon, t, q_e, q_d)$ -indistinguibilidad bajo ataques de cifrado elegido (IND-CCA, “indistinguishability under chosen-ciphertext attacks”), si cualquier adversario $\mathcal{A}$ que corre en tiempo $\leq t$, realiza $\leq q_e$ queries a $\mathcal{O}$ (one-time: $q_e = 1$) y realiza $\leq q_d$ queries a D , tiene ventaja

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

Lemma 18 (PKE OT-IND-CCA $\Rightarrow$ PKE IND-CCA). Sea $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ un PKES que ofrece $(\varepsilon, t, 1, q_d)$ -IND-CCA (i.e. OT-IND-CCA). Entonces ofrece $(q_e \cdot \varepsilon, \approx t, q_e, q_d)$ -IND-CCA con $q_e \in \mathbb{Z}_{>0}$.

Demostración. La demostración es idéntica a la de PKE OT-IND-CPA $\Rightarrow$ PKE IND-CPA, Lemma 17. $\square$

Ejemplo 10. En la practica, un oráculo de descifrado podría suceder en sistemas de cifrado de email. Un proveedor de correo electrónico “Daniel” podría modificar un correo “De Alicia para Bob: $\text{Enc}(\text{pk}_{\text{Bob}}, m)$ ” en “De Daniel para Bob: $\text{Enc}(\text{pk}_{\text{Bob}}, m)$ ”. Al responderle a Dan, Bob podría citar los contenidos originales de m , resultando en un oráculo de descifrado.

Lemma 19 (AE $\Rightarrow$ IND-CCA $\Rightarrow$ IND-CPA). La noción de seguridad IND-CCA es “intermedia” entre AE e IND-CPA.

Boceto de demostración. En ambos casos de cifrado simétrico y de clave pública, IND-CCA $\Rightarrow$ IND-CPA dado que los juegos Exp^{CPA} y Exp^{CCA} son idénticos, excepto que Exp^{CCA} le otorga menos oráculos al adversario $\mathcal{A}$. En lo siguiente suponemos un SKES es correcto. En el caso de cifrado simétrico, queremos demostrar que AE $\Rightarrow$ IND-CCA. Dado que AE requiere INT-CTXT, $\mathcal{A}$ puede solamente generar cifrados c_i válidos, tales que $\text{Dec}(k, c_i) \neq \perp$, solo a través del oráculo $E(\cdot)$ de cifrado. Esto quiere decir que si c_i es válido, $\mathcal{A}$ ya conoce el valor $m_i = \text{Dec}(k, c_i)$, dado que obtuvo c_i llamando $E(m_i)$. De otro lado, si c_i no es válido, $\mathcal{A}$ ya sabe que $\text{Dec}(k, c_i) = \perp$. Si así no fuera, $\mathcal{A}$ habría falsificado un cifrado, contradiciendo IND-CTXT y por lo tanto AE. En otras palabras, el oráculo $D(\cdot)$ no le da ninguna ventaja a $\mathcal{A}$, dado que no puede llamarlo sobre cifrados para los que ya no conozca $\text{Dec}(k, c_i)$. Si $\mathcal{A}$ tuviera uso para el oráculo $D(\cdot)$, es porque $\mathcal{A}$ podría generar cifrados c_i para los cuales prevee $m_i := \text{Dec}(k, c_i) \neq \perp$ pero no conoce m_i , contradiciendo INT-CTXT. $\square$

La noción de IND-CCA es una opción válida para proteger PKE de adversarios activos. En la practica, es mas comun que protocolos criptografico usen alguna noción (mas difícil de formalizar) de intercambio de claves autenticado (*authenticated key exchange*).

En la siguiente clase vamos a ver como obtener IND-CCA PKE, usando la metodología KEM-DEM.