Clase 18: transformada de Fujisaki-Okamoto

Fernando Virdia, versión: 0.0.1, junio 2024

Para construir un KEM OT-IND-CCA, vamos a utilizar una variante de la "transformada de Fujisaki-Okamoto" (FO, "Fujisaki-Okamoto transform"). Esta nos permite combinar un PKES que otorga IND-CPA, con dos funciones de hash, obteniendo un KEM OT-IND-CCA!

Hay muchas variantes de FO [HHK17], y esta no debe considerarse la única manera o la manera "correcta".

Definición 34 (KEM FO) *Sea $\mathcal{M}$ un conjunto finito. Sean $\Pi = (\mathsf{Gen}^\Pi, \mathsf{Enc}^\Pi, \mathsf{Dec}^\Pi)$ un PKES donde $\Pi.\mathcal{R}$ es el espacio de monedas de Enc^Π, $\Pi.\mathcal{M}$ es el de mensajes, y $\Pi.\mathcal{C}$ es el de cifrados, G una función de hash $G\colon \Pi.\mathcal{M} \to \Pi.\mathcal{R}$, H una función de hash $H\colon \Pi.\mathcal{M} \times \Pi.\mathcal{C} \to \mathcal{M}$. Definimos el KEM $\Pi' = (\mathsf{Gen}, \mathsf{Encaps}, \mathsf{Decaps})$ con espacio de claves a encapsular $\mathcal{M}$,*

$\mathsf{Gen}()$	$\mathsf{Encaps}(\mathsf{pk})$	$\mathsf{Decaps}(\mathsf{sk}, c)$
$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}^\Pi()$	$m \xleftarrow{\$} \mathcal{M}$	$m' \leftarrow \mathsf{Dec}^\Pi(\mathsf{sk}, c)$
return $(\mathsf{sk}, \mathsf{pk})$	$c \leftarrow \mathsf{Enc}^\Pi(\mathsf{pk}, m; G(m))$	**if** $m' = \perp$:
	$k \leftarrow H(m, c)$	**return** $\perp$
	return (k, c)	$c' \leftarrow \mathsf{Enc}^\Pi(\mathsf{pk}, m'; G(m'))$
		if $c' \neq c$:
		return $\perp$
		$k \leftarrow H(m', c)$
		return k

Teorema 6 (OT-IND-CPA PKE + ROM ⇒ OT-IND-CCA KEM, informal) *Sea Π, G, y H un PKES y dos funciones de hash como indicadas en Definition 34. Si Π otorga OT-IND-CPA y es "γ-spread"($\forall(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}^\Pi(), m, c : \Pr_{r \sim U(\Pi.\mathcal{R})}[\mathsf{Enc}^\Pi(\mathsf{pk}, m; r) = c] \leq \gamma$,) con $\gamma \approx 0$, y se consideran G y H como "oráculos aleatorios" (o sea, funciones muestreadas uniformemente al momento de la query, y disponibles al adversario como oráculos), entonces el FO KEM Π' construido como en Definition 34 otorga seguridad KEM OT-IND-CCA.*

Comentario 56 *Acabamos de introducir una nueva noción: "spreadness". La mayoría de los IND-CPA PKES otorgan spreadness. Si no es así, cualquier IND-CPA PKE puede ser modificado para otorgar spreadness de manera sencilla [BS23, Exercise 12.10]. ElGamal PKE es naturalmente γ-spread con $\gamma = 1/|\mathbb{G}|$.*

Demostración. Una demostración formal de esta variante FO puede obtenerse combinando Teoremas 3.2 y 3.3 en [HHK17]. □

Comentario 57 *La intuición de por que FO otorga IND-CCA es que el paso de re-cifrado dentro de* Decaps *garantiza de que cualquier cambiamiento aportado a un cifrado en transito c resultaría en $c' \neq c$ que no pasaría decapsulación.*

Con un OT-IND-CCA KEM disponible, podemos finalmente generar un OT-IND-CCA PKE, utilizando el método KEM-DEM. Junto a Lemma 18, esto resulta en IND-CCA PKE.

Teorema 7 (OT-IND-CCA KEM + AE ⇒ OT-IND-CCA PKE, informal) *Sea $\Pi = (\mathsf{Gen}, \mathsf{Encaps}, \mathsf{Decaps})$ un KEM, y $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ un SKES, tales que el espacio $\Pi.\mathcal{M}$ de claves a encapsular de Π es igual al espacio de claves $\Pi'.\mathcal{K}$ de Π', $\Pi.\mathcal{M} = \Pi'.\mathcal{K}$, y que $\mathsf{Gen}'() =$ "$k \xleftarrow{\$} \Pi'.\mathcal{K}$". Sea $\Pi^{hy} = (\mathsf{Gen}^{hy}, \mathsf{Enc}^{hy}, \mathsf{Dec}^{hy})$ el PKES obtenido de manera KEM-DEM,*

$\mathsf{Gen}^{hy}()$	$\mathsf{Enc}^{hy}(\mathsf{pk}, m)$	$\mathsf{Dec}^{hy}(\mathsf{sk}, c = (c_0, c_1))$
$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}()$	$k, c_0 \leftarrow \mathsf{Encaps}(\mathsf{pk})$	$k \leftarrow \mathsf{Decaps}(\mathsf{sk}, c_0)$
return $(\mathsf{sk}, \mathsf{pk})$	$c_1 \leftarrow \mathsf{Enc}'(k, m)$	$m' \leftarrow \mathsf{Dec}'(k, c_1)$
	$c \leftarrow (c_0, c_1)$	**return** m'
	return c	

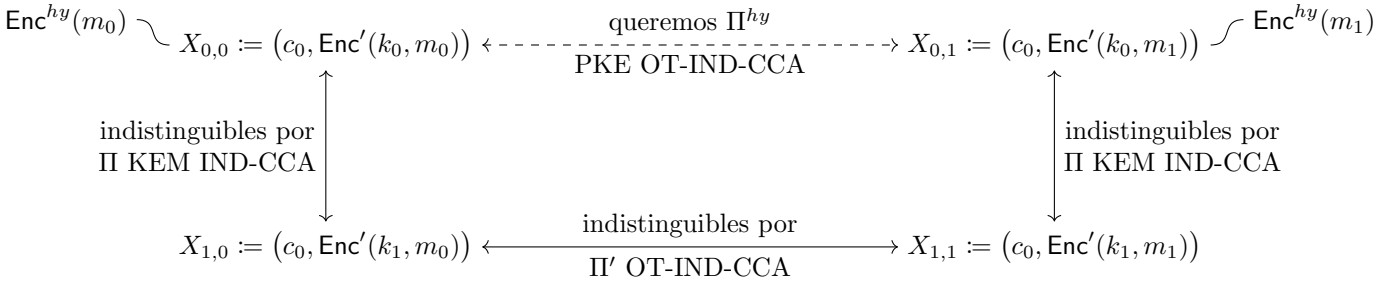
Si Π *otorga KEM OT-IND-CCA y* Π' *otorga AE, entonces* Π^{hy} *otorga PKE OT-IND-CCA.*

Comentario 58 *Para demostrar el teorema, los pasos son*

1. *demostrar que AE* $\Rightarrow$ *una noción simétrica de OT-IND-CCA.*
2. *demostrar que* Π^{hy} *otorga PKE OT-IND-CCA,*
3. *Utilizar Lemma 18 para obtener PKE IND-CCA.*

Una demostración de Item 1 se encuentra en [BS23, Theorem 9.1]. Para demostrar Item 2, la idea es de asumir un adversario $\mathcal{A}$ *que juega una variante* Exp *de* $\mathsf{Exp}^{OT\text{-}IND\text{-}CCA}$ *contra* Π^{hy} *con dos parámetros,* $\mathsf{Exp}(\mathcal{A}, b, \hat{b})$*.* $\mathcal{A}$ *tiene que adivinar* b *dado un cifrado*

$$(c_0, \mathsf{Enc}'(k_{\hat{b}}, m_b)), \text{ donde } (k_0, c_0) \leftarrow \mathsf{Encaps}(\mathsf{pk}) \text{ y } k_1 \xleftarrow{\$} \Pi.\mathcal{M} = \Pi'.\mathcal{K}.$$



Notamos que:

1. *Si* $\hat{b} = 0$*, entonces* $(c_0, \mathsf{Enc}'(k_0, m_b)) = \mathsf{Enc}^{hy}(m_b)$*, por lo que para demostrar el resultado, queremos una cota superior para la distancia entre los* $\{\mathsf{Exp}(\mathcal{A}, b, 0)\}_b$*.*
2. $X_{b,\hat{b}}$ *es una función de la variable aleatoria* $Y_{\hat{b}} \coloneqq (c_0, k_{\hat{b}})$ *(la función es* $f_{m_b}(x, y) \mapsto (x, \mathsf{Enc}'(y, m_b))$*).*
3. *Por* Π *ser un IND-CCA KEM,* $Y_{b,0}$ *y* $Y_{b,1}$ *son indistinguibles. Por* data processing inequality *(Theorem 2), también lo tienen que ser* $X_{b,0}$ *y* $X_{b,1}$*.*
4. $\mathsf{Enc}'(k_1, m_0)$ *y* $\mathsf{Enc}'(k_1, m1)$ *son indistinguibles por ser* Π' *un OT-IND-CCA SKES.*

La semejanza de $X_{0,0}$ *con* $X_{0,1}$*, de* $X_{0,1}$ *con* $X_{1,1}$ *y* $X_{1,1}$ *con* $X_{0,1}$ *nos da el resultado.*

Comentario 59 *Con los cifrados del curso, Podríamos realizar un IND-CCA PKE combinando un FO KEM basado sobre ElGamal PKE, junto a un AE obtenido como EtM. Un cifrado parecido y que también otorga IND-CCA es parte del estándar ISO/IEC 18033-2 para cifrado de claves publicas, bajo el nombre de DHIES (ECIES si* $\mathbb{G}$ *es una curva elíptica). El próximo-de-ser-estándar-FIPS ML-KEM para cifrados post-cuánticos, llamado también Kyber, es un OT-IND-CCA KEM obtenido de un tipo de postulado similar a DDH, a través de una variante de FO parecida a la que nosotros vimos.*