Yet Another Set of HACS Examples

Manuel Barbosa

February 22, 2025

1 Notes

All definitions are given for an implicit fixed value of the security parameter.

2 Definitions and Models

Game $\mathsf{IND\text{-}CCA}^{\mathsf{PKE}}_{\mathcal{A}}(b)$
$(pk, sk) \leftarrow_{\$} \mathsf{Gen}(\,)$; $c^\star \leftarrow \perp$
$(m_0, m_1, st) \leftarrow_{\$} \mathcal{A}_1^{\mathsf{ODec}(\cdot)}(pk)$
$c^\star \leftarrow_{\$} \mathsf{Enc}(pk, m_b)$
$b' \leftarrow_{\$} \mathcal{A}_2^{\mathsf{ODec}(\cdot)}(c^\star, st)$
Return b'

oracle $\mathsf{ODec}(c)$:
If $c = c^\star$ Return $\perp$
return $\mathsf{Dec}(sk, c)$

Game $\mathsf{IND\text{-}CCA}^{\mathsf{KEM}}_{\mathcal{A}}(b)$
$(pk, sk) \leftarrow_{\$} \mathsf{Gen}(\,)$
$k_1 \leftarrow_{\$} \mathcal{K}$
$(c^\star, k_0) \leftarrow_{\$} \mathsf{Enc}(pk)$
$b' \leftarrow_{\$} \mathcal{A}^{\mathsf{ODec}(\cdot)}(pk, c^\star, k_b)$
Return b'

oracle $\mathsf{ODec}(c)$:
If $c = c^\star$ Return $\perp$
return $\mathsf{Dec}(sk, c)$

Game $\mathsf{IND\text{-}CCA}^{\mathsf{DEM}}_{\mathcal{A}}(b)$
$k \leftarrow_{\$} \mathcal{K}$; $c^\star \leftarrow \perp$
$(m_0, m_1, st) \leftarrow_{\$} \mathcal{A}_1^{\mathsf{ODec}(\cdot)}(\,)$
$c^\star \leftarrow_{\$} \mathsf{Enc}(k, m_b)$
$b' \leftarrow_{\$} \mathcal{A}_2^{\mathsf{ODec}(\cdot)}(c^\star, st)$
Return b'

oracle $\mathsf{ODec}(c)$:
If $c = c^\star$ Return $\perp$
return $\mathsf{Dec}(k, c)$

Figure 1: PKE, KEM and DEM security games.

2.1 Public Key Encryption (PKE)

A PKE is defined by a secret key space $\mathcal{SK}$, a public key space $\mathcal{PK}$, a message space $\mathcal{M}$, a ciphertext space $\mathcal{C}$, and a triple of algorithms $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ as follows:

- Algorithm Gen is a distribution over key pairs $\mathcal{SK} \times \mathcal{PK}$;
- Algorithm Enc takes a public key $pk \in \mathcal{PK}$ and a message $m \in \mathcal{M}$ and outputs a ciphertext $c \in \mathcal{C}$;
- Algorithm Dec takes a secret key $sk \in \mathcal{SK}$ and a ciphertext $c \in \mathcal{C}$ and outputs either a message $m \in \mathcal{M}$ or a distinguished failure symbol $\perp$.

A PKE is (perfectly) correct if, for all $(sk, pk) \in \mathcal{SK} \times \mathcal{PK}$, all $m \in \mathcal{M}$, and all $c \in [\mathsf{Enc}(pk, m)]$, we have $\mathsf{Dec}(sk, c) = m$.

Consider the security game $\mathsf{IND\text{-}CCA}_{\mathcal{A}}^{\mathsf{PKE}}$ in Figure 1 (left).

Definition 1. *We define the advantage of an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ against* PKE *as*

$$\mathrm{Adv}_{\mathcal{A}}^{\mathsf{PKE}} := \left| \Pr\left[\mathsf{IND\text{-}CCA}_{\mathcal{A}}^{\mathsf{PKE}}(1) \Rightarrow 1 \right] - \Pr\left[\mathsf{IND\text{-}CCA}_{\mathcal{A}}^{\mathsf{PKE}}(0) \Rightarrow 1 \right] \right| .$$

2.2 Key Encapsulation Mechanism (KEM)

A KEM is defined by a secret key space $\mathcal{SK}$, a public key space $\mathcal{PK}$, a shared key space $\mathcal{K}$, a ciphertext space $\mathcal{C}$, and a triple of algorithms $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ as follows:

- Algorithm Gen is a distribution over key pairs $\mathcal{SK} \times \mathcal{PK}$;
- Algorithm Enc takes a public key $pk \in \mathcal{PK}$ and outputs a ciphertext $c \in \mathcal{C}$and a shared key $k \in \mathcal{K}$;
- Algorithm Dec takes a secret key $sk \in \mathcal{SK}$ and a ciphertext $c \in \mathcal{C}$ and outputs either a shared key $k \in \mathcal{K}$ or a distinguished failure symbol $\perp$.

A KEM is (perfectly) correct if, for all $(sk, pk) \in \mathcal{SK} \times \mathcal{PK}$, and all $(c, k) \in [\mathsf{Enc}(pk)]$, we have $\mathsf{Dec}(sk, c) = k$.

Consider the security game $\mathsf{IND\text{-}CCA}_{\mathcal{A}}^{\mathsf{KEM}}$ in Figure 1 (center).

Definition 2. *We define the advantage of an adversary $\mathcal{A}$ against* KEM *as*

$$\mathrm{Adv}_{\mathcal{A}}^{\mathsf{KEM}} := \left| \Pr\left[\mathsf{IND\text{-}CCA}_{\mathcal{A}}^{\mathsf{KEM}}(1) \Rightarrow 1 \right] - \Pr\left[\mathsf{IND\text{-}CCA}_{\mathcal{A}}^{\mathsf{KEM}}(0) \Rightarrow 1 \right] \right| .$$

2.3 Data Encapsulation Mechanism (DEM)

A DEM is defined by a key space $\mathcal{K}$ a message space $\mathcal{M}$, a ciphertext space $\mathcal{C}$, and a triple of algorithms $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ as follows:

- Algorithm Gen is a distribution over keys $\mathcal{K}$;
- Algorithm Enc takes a key $k \in \mathcal{K}$ and a message $m \in \mathcal{M}$ and outputs a ciphertext $c \in \mathcal{C}$;
- Algorithm Dec takes a key $k \in \mathcal{K}$ and a ciphertext $c \in \mathcal{C}$ and outputs either a message $m \in \mathcal{M}$ or a distinguished failure symbol $\perp$.

A DEM is (perfectly) correct if, for all $k \in \mathcal{K}$, all $m \in \mathcal{M}$, and all $c \in [\mathsf{Enc}(k, m)]$, we have $\mathsf{Dec}(k, c) = m$.

Consider the security game $\mathsf{IND\text{-}CCA}_{\mathcal{A}}^{\mathsf{DEM}}$ in Figure 1 (right).

Definition 3. *We define the advantage of an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ against* DEM *as*

$$\mathrm{Adv}_{\mathcal{A}}^{\mathsf{DEM}} := \left| \Pr\left[\mathsf{IND\text{-}CCA}_{\mathcal{A}}^{\mathsf{DEM}}(1) \Rightarrow 1 \right] - \Pr\left[\mathsf{IND\text{-}CCA}_{\mathcal{A}}^{\mathsf{DEM}}(0) \Rightarrow 1 \right] \right| .$$

3 Constructions and Proofs

3.1 KEM + DEM ⇒ PKE

Given a KEM and a DEM in which the shared key space produced by the KEM matches the key space of the DEM we can construct a PKE as shown in Figure 2.

$\underline{\mathsf{PKE.Gen}(\,)}$	$\underline{\mathsf{PKE.Enc}(pk, m)}$:	$\underline{\mathsf{PKE.Dec}(sk, c)}$:
$(pk, sk) \leftarrow_\$ \mathsf{KEM.Gen}(\,)$	$(k, c_1) \leftarrow_\$ \mathsf{KEM.Enc}(pk)$	$(c_1, c_2) \leftarrow c$
Return (pk, sk)	$c_2 \leftarrow_\$ \mathsf{DEM.Enc}(k, m)$	$k \leftarrow \mathsf{KEM.Dec}(sk, c_1)$
	Return (c_1, c_2)	If $k = \perp$ Return $\perp$
		$m \leftarrow \mathsf{DEM.Dec}(k, c_2)$
		Return m

Figure 2: KEM+DEM construction.

Theorem 1. *If KEM is perfectly correct, then the advantage of any attacker $\mathcal{A}$ against the KEM+DEM construction is bounded as follows, where adversaries $\mathcal{B}_1^0$, $\mathcal{B}_1^1$ and $\mathcal{B}_2$ are shown in Figure 4.*

$$\mathrm{Adv}_{\mathcal{A}}^{\mathsf{PKE}} \leq \mathrm{Adv}_{\mathcal{B}_1^0}^{\mathsf{KEM}} + \mathrm{Adv}_{\mathcal{B}_1^1}^{\mathsf{KEM}} + \mathrm{Adv}_{\mathcal{B}_2}^{\mathsf{DEM}} .$$

Proof. The proof proceeds as a sequence of games, as shown in Figure 3:

- The first game, on the left, is the PKE security game instantiated with the KEM+DEM construction.
- The second game $\mathsf{G1}$ introduces two modifications: the KEM challenge ciphertext $c_1^\star$ is generated upfront, and the decryption oracle never decrypts $c_1^\star$ it, using $k^\star$ as the assumed result instead. Since the KEM is perfectly correct, these modifications are not noticeable by the adversary and we have that

  $$\mathrm{Adv}_{\mathcal{A}}^{\mathsf{PKE}} = \left| \Pr\left[\, \mathsf{G1}_{\mathcal{A}}^{\mathsf{PKE}}(1) \Rightarrow 1 \,\right] - \Pr\left[\, \mathsf{G1}_{\mathcal{A}}^{\mathsf{PKE}}(0) \Rightarrow 1 \,\right] \right|$$

  Note also that $k^\star \neq \perp$ also because of KEM correctness.
- The third and final game $\mathsf{G2}$ introduces one modification: $k^\star$ is replaced with a random key. To bound the impact of this change in the adversary's view, we rely on adversaries $\mathcal{B}_1^0$ and $\mathcal{B}_1^1$, which attack the KEM security game. These adversaries interpolate perfectly between games $\mathsf{G1}$ and $\mathsf{G2}$ in that, for $b = 0, 1$, it is easy to see that:

  $$\Pr\left[\, \mathsf{G1}_{\mathcal{A}}^{\mathsf{PKE}}(b) \Rightarrow 1 \,\right] \;=\; \Pr\left[\, \mathsf{IND\text{-}CCA}_{\mathcal{B}_1^b}^{\mathsf{KEM}}(0) \Rightarrow 1 \,\right]$$

  $$\Pr\left[\, \mathsf{G2}_{\mathcal{A}}^{\mathsf{PKE}}(b) \Rightarrow 1 \,\right] \;=\; \Pr\left[\, \mathsf{IND\text{-}CCA}_{\mathcal{B}_1^b}^{\mathsf{KEM}}(1) \Rightarrow 1 \,\right]$$
- We now bound the adversary's advantage in the final game using DEM security. We construct adversary $\mathcal{B}_2$, with the following property for $b = 0, 1$:

  $$\Pr\left[\, \mathsf{G2}_{\mathcal{A}}^{\mathsf{PKE}}(b) \Rightarrow 1 \,\right] \;=\; \Pr\left[\, \mathsf{IND\text{-}CCA}_{\mathcal{B}_2}^{\mathsf{DEM}}(b) \Rightarrow 1 \,\right]$$

- We now put everything together to conclude the proof:

$$
\begin{aligned}
\mathrm{Adv}^{\mathsf{PKE}}_{\mathcal{A}} &= \left| \Pr\left[\,\mathsf{G1}^{\mathsf{PKE}}_{\mathcal{A}}(1) \Rightarrow 1\,\right] - \Pr\left[\,\mathsf{G1}^{\mathsf{PKE}}_{\mathcal{A}}(0) \Rightarrow 1\,\right] \right| \\
&= \Big| \Pr\left[\,\mathsf{G1}^{\mathsf{PKE}}_{\mathcal{A}}(1) \Rightarrow 1\,\right] - \Pr\left[\,\mathsf{G2}^{\mathsf{PKE}}_{\mathcal{A}}(1) \Rightarrow 1\,\right] + \\
&\qquad \Pr\left[\,\mathsf{G2}^{\mathsf{PKE}}_{\mathcal{A}}(1) \Rightarrow 1\,\right] - \Pr\left[\,\mathsf{G2}^{\mathsf{PKE}}_{\mathcal{A}}(0) \Rightarrow 1\,\right] + \\
&\qquad \Pr\left[\,\mathsf{G2}^{\mathsf{PKE}}_{\mathcal{A}}(0) \Rightarrow 1\,\right] - \Pr\left[\,\mathsf{G1}^{\mathsf{PKE}}_{\mathcal{A}}(0) \Rightarrow 1\,\right] \Big| \\
&\leq \left| \Pr\left[\,\mathsf{G1}^{\mathsf{PKE}}_{\mathcal{A}}(1) \Rightarrow 1\,\right] - \Pr\left[\,\mathsf{G2}^{\mathsf{PKE}}_{\mathcal{A}}(1) \Rightarrow 1\,\right] \right| + \\
&\qquad \left| \Pr\left[\,\mathsf{G2}^{\mathsf{PKE}}_{\mathcal{A}}(1) \Rightarrow 1\,\right] - \Pr\left[\,\mathsf{G2}^{\mathsf{PKE}}_{\mathcal{A}}(0) \Rightarrow 1\,\right] \right| + \\
&\qquad \left| \Pr\left[\,\mathsf{G2}^{\mathsf{PKE}}_{\mathcal{A}}(0) \Rightarrow 1\,\right] - \Pr\left[\,\mathsf{G1}^{\mathsf{PKE}}_{\mathcal{A}}(0) \Rightarrow 1\,\right] \right| \\
&= \left| \Pr\left[\,\mathsf{IND\text{-}CCA}^{\mathsf{KEM}}_{\mathcal{B}_1^1}(0) \Rightarrow 1\,\right] - \Pr\left[\,\mathsf{IND\text{-}CCA}^{\mathsf{KEM}}_{\mathcal{B}_1^1}(1) \Rightarrow 1\,\right] \right| + \\
&\qquad \left| \Pr\left[\,\mathsf{IND\text{-}CCA}^{\mathsf{DEM}}_{\mathcal{B}_2}(1) \Rightarrow 1\,\right] - \Pr\left[\,\mathsf{IND\text{-}CCA}^{\mathsf{DEM}}_{\mathcal{B}_2}(0) \Rightarrow 1\,\right] \right| + \\
&\qquad \left| \Pr\left[\,\mathsf{IND\text{-}CCA}^{\mathsf{KEM}}_{\mathcal{B}_1^0}(1) \Rightarrow 1\,\right] - \Pr\left[\,\mathsf{IND\text{-}CCA}^{\mathsf{KEM}}_{\mathcal{B}_1^0}(0) \Rightarrow 1\,\right] \right|
\end{aligned}
$$

□

Game $\mathsf{IND\text{-}CCA}^{\mathsf{PKE}}_{\mathcal{A}}(b)$	Game $\mathsf{G1}^{\mathsf{PKE}}_{\mathcal{A}}(b)$	Game $\mathsf{G2}^{\mathsf{PKE}}_{\mathcal{A}}(b)$
$(pk, sk) \leftarrow_{\$} \mathsf{KEM.Gen}(\,);\ c^\star \leftarrow \perp$	$(pk, sk) \leftarrow_{\$} \mathsf{KEM.Gen}(\,);\ c^\star \leftarrow \perp$	$(pk, sk) \leftarrow_{\$} \mathsf{KEM.Gen}(\,);\ c^\star \leftarrow \perp$
$(m_0, m_1, st) \leftarrow_{\$} \mathcal{A}_1^{\mathsf{ODec}(\cdot)}(pk)$	$(k^\star, c_1^\star) \leftarrow_{\$} \mathsf{KEM.Enc}(pk)$	$(\_, c_1^\star) \leftarrow_{\$} \mathsf{KEM.Enc}(pk);\ k^\star \leftarrow_{\$} \mathcal{K}$
$(k^\star, c_1^\star) \leftarrow_{\$} \mathsf{KEM.Enc}(pk)$	$(m_0, m_1, st) \leftarrow_{\$} \mathcal{A}_1^{\mathsf{ODec}(\cdot)}(pk)$	$(m_0, m_1, st) \leftarrow_{\$} \mathcal{A}_1^{\mathsf{ODec}(\cdot)}(pk)$
$c_2^\star \leftarrow_{\$} \mathsf{DEM.Enc}(k^\star, m_b)$	$c_2^\star \leftarrow_{\$} \mathsf{DEM.Enc}(k^\star, m_b)$	$c_2^\star \leftarrow_{\$} \mathsf{DEM.Enc}(k^\star, m_b)$
$c^\star \leftarrow (c_1^\star, c_2^\star)$	$c^\star \leftarrow (c_1^\star, c_2^\star)$	$c^\star \leftarrow (c_1^\star, c_2^\star)$
$b' \leftarrow_{\$} \mathcal{A}_2^{\mathsf{ODec}(\cdot)}(c^\star, st)$	$b' \leftarrow_{\$} \mathcal{A}_2^{\mathsf{ODec}(\cdot)}(c^\star, st)$	$b' \leftarrow_{\$} \mathcal{A}_2^{\mathsf{ODec}(\cdot)}(c^\star, st)$
Return b'	Return b'	Return b'
oracle $\mathsf{ODec}(c)$:	oracle $\mathsf{ODec}(c)$:	oracle $\mathsf{ODec}(c)$:
If $c = c^\star$ Return $\perp$	If $c = c^\star$ Return $\perp$	If $c = c^\star$ Return $\perp$
$(c_1, c_2) \leftarrow c$	$(c_1, c_2) \leftarrow c$	$(c_1, c_2) \leftarrow c$
	If $c_1 = c_1^\star$	If $c_1 = c_1^\star$
	Then:	Then:
	$k \leftarrow k_\star$	$k \leftarrow k_\star$
	$m \leftarrow \mathsf{DEM.Dec}(k, c_2)$	$m \leftarrow \mathsf{DEM.Dec}(k, c_2)$
	Else	Else
$k \leftarrow \mathsf{KEM.Dec}(sk, c_1)$	$k \leftarrow \mathsf{KEM.Dec}(sk, c_1)$	$k \leftarrow \mathsf{KEM.Dec}(sk, c_1)$
If $k = \perp$ Return $\perp$	If $k = \perp$ Return $\perp$	If $k = \perp$ Return $\perp$
$m \leftarrow \mathsf{DEM.Dec}(k, c_2)$	$m \leftarrow \mathsf{DEM.Dec}(k, c_2)$	$m \leftarrow \mathsf{DEM.Dec}(k, c_2)$
Return m	Return m	Return m

Figure 3: KEM+DEM sequence of games.

Variants/exercises:

Adversary $\mathcal{B}_1^b(pk, c_1^\star, k^\star)$

$c^\star \leftarrow \perp$
$(m_0, m_1, st) \leftarrow_\$ \mathcal{A}_1^{\mathsf{ODec}(\cdot)}(pk)$
$c_2^\star \leftarrow_\$ \mathsf{DEM.Enc}(k^\star, m_b)$
$c^\star \leftarrow (c_1^\star, c_2^\star)$
$b' \leftarrow_\$ \mathcal{A}_2^{\mathsf{ODec}(\cdot)}(c^\star, st)$
Return b'

oracle $\mathsf{ODec}(c)$:

If $c = c^\star$ Return $\perp$
$(c_1, c_2) \leftarrow c$
If $c_1 = c_1^\star$
Then:
  $k \leftarrow k_\star$
  $m \leftarrow \mathsf{DEM.Dec}(k, c_2)$
Else
  Call $\mathsf{ODec}(c_1)$ to get k
  If $k = \perp$ Return $\perp$
  $m \leftarrow \mathsf{DEM.Dec}(k, c_2)$
Return m

Adversary $\mathcal{B}_{2,1}(\,)$

$(pk, sk) \leftarrow_\$ \mathsf{KEM.Gen}(\,)$; $c^\star \leftarrow \perp$
$(\_, c_1^\star) \leftarrow_\$ \mathsf{KEM.Enc}(pk)$
$(m_0, m_1, st_{\mathcal{A}}) \leftarrow_\$ \mathcal{A}_1^{\mathsf{ODec}(\cdot)}(pk)$
Return $(m_0, m_1, (st_{\mathcal{A}}, sk, c_1^\star))$

Adversary $\mathcal{B}_{2,2}(c_2^\star, st)$

$(st_{\mathcal{A}}, sk, c_1^\star) \leftarrow st$
$c^\star \leftarrow (c_1^\star, c_2^\star)$
$b' \leftarrow_\$ \mathcal{A}_2^{\mathsf{ODec}(\cdot)}(c^\star, st_{\mathcal{A}})$
Return b'

oracle $\mathsf{ODec}(c)$:

If $c = c^\star$ Return $\perp$
$(c_1, c_2) \leftarrow c$
If $c_1 = c_1^\star$
Then:
  Call $\mathsf{ODec}(c_2)$ to get m
Else
  $k \leftarrow \mathsf{KEM.Dec}(sk, c_1)$
  If $k = \perp$ Return $\perp$
  $m \leftarrow \mathsf{DEM.Dec}(k, c_2)$
Return m

Figure 4: KEM+DEM adversaries: $\mathcal{B}_1^b$ for $b = 0, 1$ attack KEM security; $\mathcal{B}_2 = (\mathcal{B}_{2,1}, \mathcal{B}_{2,2})$ attacks DEM security. Both use $\mathcal{A}$ as a subroutine.

- CPA variant: if either or both KEM and DEM are only CPA secure, then the resulting PKE is CPA secure. In the proof, there is no need for the correctness hop.

- RO variant: suppose either or both KEM and DEM are proved secure in the Random Oracle Model (ROM) wrt to independent H_{KEM} and H_{DEM}. Then the resulting PKE is secure in the ROM, with the adversary having access to both H_{KEM} and H_{DEM}.

- Imperfect correctness: if the KEM is not perfectly correct, then the first step in the above proof needs to be modified to account for this loss using an up-to-bad argument. The bad event is activated if decrypting $c_1^\star$ results in something other than $k^\star$.