Hybrid encryption

- Asymmetric encryption uses number-theoretic operations and is slower than symmetric encryption that often uses block ciphers.
- Also we often want to encrypt long messages.
- In practice one usually
  1. encrypts a randomly chosen symmetric key K using an asymmetric encryption algorithm and then
  2. encrypts a message using a symmetric encryption algorithm and K.
- This is called hybrid encryption

Hybrid encryption

- Let $\mathcal{AE} = (\mathcal{K}^a, \mathcal{E}^a, \mathcal{D}^a)$ be an asymmetric encryption scheme and let $\mathcal{SE} = (\mathcal{K}^s, \mathcal{E}^s, \mathcal{D}^s)$ be a symmetric encryption scheme, s.t. the set of keys for $\mathcal{SE}$ is always in the message space of $\mathcal{AE}$.

  Then the associated hybrid scheme $\overline{\mathcal{AE}} = (\mathcal{K}^a, \overline{\mathcal{E}}, \overline{\mathcal{D}})$ is as follows:

Algorithm $\overline{\mathcal{E}}_{pk}(M)$	Algorithm $\overline{\mathcal{D}}_{sk}(C)$
$K \xleftarrow{\$} \mathcal{K}^s$; $C^s \xleftarrow{\$} \mathcal{E}^s_K(M)$	Parse C as (C^a, C^s)
If $C^s = \perp$ then return $\perp$	$K \leftarrow \mathcal{D}^a_{sk}(C^a)$
$C^a \xleftarrow{\$} \mathcal{E}^a_{pk}(K)$; $C \leftarrow (C^a, C^s)$	If $K = \perp$ then return $\perp$
Return C	$M \leftarrow \mathcal{D}^s_K(C^s)$
	Return M

- Note that the hybrid scheme is an asymmetric encryption scheme

Hybrid encryption

- <u>Theorem</u>. Let $\mathcal{AE} = (\mathcal{K}^a, \mathcal{E}^a, \mathcal{D}^a)$ be an asymmetric encryption scheme and let $\mathcal{SE} = (\mathcal{K}^s, \mathcal{E}^s, \mathcal{D}^s)$ be a symmetric encryption scheme, s.t. the set of keys for $\mathcal{SE}$ is always in the message space of $\mathcal{AE}$. Let $\overline{\mathcal{AE}} = (\mathcal{K}^a, \overline{\mathcal{E}}, \overline{\mathcal{D}})$ be the associated hybrid scheme as defined on the previous slide. Then for any adversary *B* there exist adversaries $A_{00,01}$, $A_{00,01}$, *A* s.t.

$$\mathbf{Adv}^{\text{ind-cpa}}_{\overline{\mathcal{AE}}}(B)$$

$$\leq \mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{AE}}(A_{00,01}) + \mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{AE}}(A_{11,10}) + q\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A)$$

and $A_{00,01}$, $A_{10,11}$ have time complexity of *B*, make the same number of queries, each of length k (symmetric key length), and A has time complexity of *B* and makes only one query.

- <u>Collorary</u>. If the components are IND-CPA, then the associated hybrid scheme is also IND-CPA.

- <u>Proof</u>. The proof will use a hybrid argument. We will define a sequence of 4 experiments associated with *B*

$$\mathbf{Exp}^{00}_{\overline{\mathcal{AE}}}(B)\ ,\ \mathbf{Exp}^{01}_{\overline{\mathcal{AE}}}(B)\ ,\ \mathbf{Exp}^{11}_{\overline{\mathcal{AE}}}(B)\ ,\ \mathbf{Exp}^{10}_{\overline{\mathcal{AE}}}(B)$$

and define

$$P(\alpha, \beta) \;=\; \Pr\left[\mathbf{Exp}^{\alpha\beta}_{\overline{\mathcal{AE}}}(B) = 1\right]$$

It will be the case that

$$P(1,0) \;=\; \Pr\left[\mathbf{Exp}^{\text{ind-cpa-1}}_{\overline{\mathcal{AE}}}(B) = 1\right]$$

$$P(0,0) \;=\; \Pr\left[\mathbf{Exp}^{\text{ind-cpa-0}}_{\overline{\mathcal{AE}}}(B) = 1\right]$$

and thus

$$\begin{aligned} \mathbf{Adv}^{\text{ind-cpa}}_{\overline{\mathcal{AE}}}(B) &= P(1,0) - P(0,0) \\ &= P(1,0) - P(1,1) + P(1,1) - P(0,1) + P(0,1) - P(0,0) \\ &= [P(1,0) - P(1,1)] + [P(1,1) - P(0,1)] + [P(0,1) - P(0,0)] \end{aligned}$$

We will construct adversaries $A_{00,01}$, A, $A_{00,01}$ s.t.

$$
\begin{aligned}
P(0,1) - P(0,0) &\leq \mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{AE}}(A_{01,00}) \\
P(1,1) - P(0,1) &\leq \mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) \\
P(1,0) - P(1,1) &\leq \mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{AE}}(A_{10,11})
\end{aligned}
$$

and the theorem statement will follow.

We now define the 4 experiments that use different oracles

$\mathcal{HE}^{00}_{pk}(\cdot,\cdot)$, $\mathcal{HE}^{01}_{pk}(\cdot,\cdot)$, $\mathcal{HE}^{11}_{pk}(\cdot,\cdot)$, $\mathcal{HE}^{10}_{pk}(\cdot,\cdot)$

For all possible bits α, β define

Experiment $\mathbf{Exp}^{\alpha\beta}_{\mathcal{AE}}(B)$
$(pk, sk) \xleftarrow{\$} \mathcal{K}^a$
$d \leftarrow B^{\mathcal{HE}^{\alpha\beta}_{pk}(\cdot,\cdot)}(pk)$
Return d

Oracle $\mathcal{HE}^{00}_{pk}(M_0, M_1)$ $K_0 \xleftarrow{\$} \mathcal{K}^s$; $K_1 \xleftarrow{\$} \mathcal{K}^s$ $C^s \xleftarrow{\$} \mathcal{E}^s(K_0, \boxed{M_0})$ If $C^s = \perp$ then return $\perp$ $C^a \xleftarrow{\$} \mathcal{E}^a(pk, \boxed{K_0})$ $C \leftarrow (C^a, C^s)$ Return C	Oracle $\mathcal{HE}^{01}_{pk}(M_0, M_1)$ $K_0 \xleftarrow{\$} \mathcal{K}^s$; $K_1 \xleftarrow{\$} \mathcal{K}^s$ $C^s \xleftarrow{\$} \mathcal{E}^s(K_0, \boxed{M_0})$ If $C^s = \perp$ then return $\perp$ $C^a \xleftarrow{\$} \mathcal{E}^a(pk, \boxed{K_1})$ $C \leftarrow (C^a, C^s)$ Return C
Oracle $\mathcal{HE}^{11}_{pk}(M_0, M_1)$ $K_0 \xleftarrow{\$} \mathcal{K}^s$; $K_1 \xleftarrow{\$} \mathcal{K}^s$ $C^s \xleftarrow{\$} \mathcal{E}^s(K_0, \boxed{M_1})$ If $C^s = \perp$ then return $\perp$ $C^a \xleftarrow{\$} \mathcal{E}^a(pk, \boxed{K_1})$ $C \leftarrow (C^a, C^s)$ Return C	Oracle $\mathcal{HE}^{10}_{pk}(M_0, M_1)$ $K_0 \xleftarrow{\$} \mathcal{K}^s$; $K_1 \xleftarrow{\$} \mathcal{K}^s$ $C^s \xleftarrow{\$} \mathcal{E}^s(K_0, \boxed{M_1})$ If $C^s = \perp$ then return $\perp$ $C^a \xleftarrow{\$} \mathcal{E}^a(pk, \boxed{K_0})$ $C \leftarrow (C^a, C^s)$ Return C

Check that

$$
\begin{aligned}
P(1,0) &= \Pr\left[\mathbf{Exp}^{\text{ind-cpa-1}}_{\mathcal{AE}}(B) = 1\right] \\
P(0,0) &= \Pr\left[\mathbf{Exp}^{\text{ind-cpa-0}}_{\mathcal{AE}}(B) = 1\right]
\end{aligned}
$$

We now construct adversaries $A_{00,01}$, $A_{10,11}$

Adversary $A_{01,00}^{\mathcal{E}^a_{pk}(\mathrm{LR}(\cdot,\cdot,b))}(pk)$ Subroutine $\mathcal{OE}(M_0, M_1)$ $K_0 \xleftarrow{\$} \mathcal{K}^s$; $K_1 \xleftarrow{\$} \mathcal{K}^s$ $C^s \xleftarrow{\$} \mathcal{E}^s(K_0, M_0)$ If $C^s = \perp$ then return $\perp$ $C^a \xleftarrow{\$} \mathcal{E}^a_{pk}(\mathrm{LR}(K_0, K_1, b))$ Return (C^a, C^s) End Subroutine $d \xleftarrow{\$} B^{\mathcal{OE}(\cdot,\cdot)}(pk)$ Return d	Adversary $A_{10,11}^{\mathcal{E}^a_{pk}(\mathrm{LR}(\cdot,\cdot,b))}(pk)$ Subroutine $\mathcal{OE}(M_0, M_1)$ $K_0 \xleftarrow{\$} \mathcal{K}^s$; $K_1 \xleftarrow{\$} \mathcal{K}^s$ $C^s \xleftarrow{\$} \mathcal{E}^s(K_0, M_1)$ If $C^s = \perp$ then return $\perp$ $C^a \xleftarrow{\$} \mathcal{E}^a_{pk}(\mathrm{LR}(K_1, K_0, b))$ Return (C^a, C^s) End Subroutine $d \xleftarrow{\$} B^{\mathcal{OE}(\cdot,\cdot)}(pk)$ Return d

Check that

$$
\begin{aligned}
\Pr\left[\mathbf{Exp}^{\text{ind-cpa-1}}_{\mathcal{AE}}(A_{01,00}) = 1\right] &= \Pr\left[\mathbf{Exp}^{01}_{\mathcal{AE}}(B) = 1\right] \\
\Pr\left[\mathbf{Exp}^{\text{ind-cpa-0}}_{\mathcal{AE}}(A_{01,00}) = 1\right] &= \Pr\left[\mathbf{Exp}^{00}_{\mathcal{AE}}(B) = 1\right]
\end{aligned}
$$

$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{AE}}(A_{01,00}) = P(0,1) - P(0,0)$$

Similarly for $A_{10,11}$

We now construct A. As A can make only 1 query, the construction will require another sequence of hybrid arguments

$$\mathbf{Exp}^{0}_{\mathcal{AE}}(B)\ ,\ \ \mathbf{Exp}^{1}_{\mathcal{AE}}(B)\ ,\ \ \ldots\ ,\ \ \mathbf{Exp}^{q}_{\mathcal{AE}}(B)$$

Define $P(i) \ = \ \Pr\left[\mathbf{Exp}^{i}_{\mathcal{AE}}(B) = 1\right]$

Oracle $\mathcal{HE}^{\,i}_{pk}(M_0, M_1)$

$j \leftarrow j + 1$

$K_0 \xleftarrow{\$} \mathcal{K}^s$; $K_1 \xleftarrow{\$} \mathcal{K}^s$

If $j \leq i$

then $C^s \xleftarrow{\$} \mathcal{E}^s(K_0, \boxed{M_1})$

else $C^s \xleftarrow{\$} \mathcal{E}^s(K_0, \boxed{M_0})$

EndIf

If $C^s = \perp$ then return $\perp$

$C^a \xleftarrow{\$} \mathcal{E}^a(pk, \boxed{K_1})$

$C \leftarrow (C^a, C^s)$

Return C

Experiment $\mathbf{Exp}^{i}_{\mathcal{AE}}(B)$

$(pk, sk) \xleftarrow{\$} \mathcal{K}^a$

$d \leftarrow B^{\mathcal{HE}^{\,i}_{pk}(\cdot,\cdot)}(pk)$

Return d

Check that

$P(0,1) = P(0) \quad$ and $\quad P(1,1) = P(q)$

$P(1,1) - P(0,1)$

$$\begin{aligned} &= P(q) - P(0) \\ &= P(q) - P(q-1) + P(q-1) - \cdots - P(1) + P(1) - P(0) \\ &= \sum_{i=1}^{q} [P(i) - P(i-1)]\ . \end{aligned}$$

Adversary $A^{\mathcal{E}^s_K(\mathrm{LR}(\cdot,\cdot,b))}$

$(pk, sk) \xleftarrow{\$} \mathcal{K}^a$; $j \leftarrow 0$; $I \xleftarrow{\$} \{1, \ldots, q\}$

Subroutine $\mathcal{OE}(M_0, M_1)$

$j \leftarrow j + 1$

$K_0 \xleftarrow{\$} \mathcal{K}^s$; $K_1 \xleftarrow{\$} \mathcal{K}^s$

If $j < I$ then $C^s \xleftarrow{\$} \mathcal{E}^s(K_0, \boxed{M_1})$ EndIf

If $j = I$ then $C^s \xleftarrow{\$} \mathcal{E}^s_K(\mathrm{LR}(M_0, M_1, b))$ EndIf

If $j > I$ then $C^s \xleftarrow{\$} \mathcal{E}^s(K_0, \boxed{M_0})$ EndIf

If $C^s = \perp$ then return $\perp$

$C^a \xleftarrow{\$} \mathcal{E}^a(pk, \boxed{K_1})$

Return (C^a, C^s)

End Subroutine

$d \xleftarrow{\$} B^{\mathcal{OE}(\cdot,\cdot)}(pk)$

Return d

Check that

$$\Pr\left[\mathbf{Exp}^{\text{ind-cpa-1}}_{\mathcal{SE}}(A) = 1 \mid I = i\right] \ = \ P(i)$$

$$\Pr\left[\mathbf{Exp}^{\text{ind-cpa-0}}_{\mathcal{SE}}(A) = 1 \mid I = i\right] \ = \ P(i-1)$$

Analyzing A we get

$\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A)$

$$\begin{aligned} &= \Pr\left[\mathbf{Exp}^{\text{ind-cpa-1}}_{\mathcal{SE}}(A) = 1\right] - \Pr\left[\mathbf{Exp}^{\text{ind-cpa-0}}_{\mathcal{SE}}(A) = 1\right] \\ &= \sum_{i=1}^{q} \Pr\left[\mathbf{Exp}^{\text{ind-cpa-1}}_{\mathcal{SE}}(A) = 1 \mid I = i\right] \cdot \Pr[I = i] \\ &\qquad - \sum_{i=1}^{q} \Pr\left[\mathbf{Exp}^{\text{ind-cpa-0}}_{\mathcal{SE}}(A) = 1 \mid I = i\right] \cdot \Pr[I = i] \\ &= \sum_{i=1}^{q} P(i) \cdot \Pr[I = i] \ - \ \sum_{i=1}^{q} P(i-1) \cdot \Pr[I = i] \\ &= \frac{1}{q} \cdot \sum_{i=1}^{q} P(i) - P(i-1) \\ &= \frac{1}{q} \cdot [P(1,1) - P(0,1)]\ . \end{aligned}$$

- Note that a symmetric encryption scheme can satisfy a definition weaker than IND-CPA (as in the proof *A* makes only one query to the LR oracle.)
  - In particular, the symmetric scheme can be deterministic
  - This is because a new symmetric key is picked for each message
- An analogues theorem can be stated and proved for the case of chosen-ciphertext attacks (if the components are IND-CCA secure, then the hybrid scheme is IND-CCA secure).