Advanced Cryptography

Spring Semester 2021

Homework 2

Rolin Nicolas, Leclair Louis

1 Introduction to Random Oracles

Question 1. We simply change H to :

```
Oracle: H(x)
// before first query
S ←()
// on a query
if (x, y) ∈ S then
 |  return y
end
sample y uniformly from {0,1}^{l_2}
S ←(x,y)
return y
```

Question 2. If $\Pr[\overline{query}] = 0$ then $\Pr[query] = 1$ and we trivially have :

$$|\Pr[\Gamma^0(\mathcal{A}) \implies 1] - \Pr[\Gamma^1(\mathcal{A}) \implies 1]| \leq 1 = \Pr[query]$$

If $\Pr[\overline{query}] > 0$:

The sampling is uniformly random so an adversary only gets information on y if he queries x to H. So the adversary cannot distinguish between Γ^0 and Γ^1 if the event *query* does not happen which implies that :

$$\Pr[\Gamma^0(\mathcal{A}) \implies 1|\overline{query}] = \Pr[\Gamma^1(\mathcal{A}) \implies 1|\overline{query}]$$
$$\frac{\Pr[\Gamma^0(\mathcal{A}) \implies 1 \cap \overline{query}]}{\Pr[\overline{query}]} = \frac{\Pr[\Gamma^1(\mathcal{A}) \implies 1 \cap \overline{query}]}{\Pr[\overline{query}]}$$

$$\Pr[\Gamma^0(\mathcal{A}) \implies 1 \cap \overline{query}] = \Pr[\Gamma^1(\mathcal{A}) \implies 1 \cap \overline{query}] \tag{1}$$

Using (1) we can now deduce the inequality :

$$\Pr[\Gamma^0(\mathcal{A}) \implies 1] = \Pr[\Gamma^0(\mathcal{A}) \implies 1 \cap query] + \Pr[\Gamma^0(\mathcal{A}) \implies 1 \cap \overline{query}]$$
$$\Pr[\Gamma^0(\mathcal{A}) \implies 1] = \Pr[\Gamma^0(\mathcal{A}) \implies 1 \cap query] + \Pr[\Gamma^1(\mathcal{A}) \implies 1 \cap \overline{query}]$$
$$\Pr[\Gamma^0(\mathcal{A}) \implies 1] \leq \Pr[\Gamma^0(\mathcal{A}) \implies 1 \cap query] + \Pr[\Gamma^1(\mathcal{A}) \implies 1 \cap \overline{query}] + \Pr[\Gamma^1(\mathcal{A}) \implies 1 \cap query]$$
$$\Pr[\Gamma^0(\mathcal{A}) \implies 1] \leq \Pr[\Gamma^0(\mathcal{A}) \implies 1 \cap query] + \Pr[\Gamma^1(\mathcal{A}) \implies 1]$$
$$\Pr[\Gamma^0(\mathcal{A}) \implies 1] \leq \Pr[query] + \Pr[\Gamma^1(\mathcal{A}) \implies 1]$$

At last we get :

$$\Pr[\Gamma^0(\mathcal{A}) \implies 1] - \Pr[\Gamma^1(\mathcal{A}) \implies 1] \leq \Pr[query] \tag{2}$$

This the same kind of logic we get :

$$\Pr[\Gamma^1(\mathcal{A}) \implies 1] - \Pr[\Gamma^0(\mathcal{A}) \implies 1] \leq \Pr[query] \tag{3}$$

Combining (2) and (3) we get :

$$|\Pr[\Gamma^0(\mathcal{A}) \implies 1] - \Pr[\Gamma^1(\mathcal{A}) \implies 1]| \leq \Pr[query]$$

Which is what we have to demonstrate.

Question 3. a)

Game: $\mathsf{IND\text{-}CPA}^0_{\mathsf{KEM}}(\mathcal{A})$	**Game:** $\mathsf{IND\text{-}CPA}^1_{\mathsf{KEM}}(\mathcal{A})$
(pk, sk) $\leftarrow_\$ Gen(1^\lambda)$	(pk, sk) $\leftarrow_\$ Gen(1^\lambda)$
pt $\leftarrow_\$ \{0,1\}^{l_2}$	pt $\leftarrow_\$ \{0,1\}^{l_2}$
ct* $\leftarrow enc(pk, pt)$	ct* $\leftarrow enc(pk, pt)$
K* $\leftarrow H(pt)$	K $\leftarrow H(pt)$
b' $\leftarrow_\$ \mathcal{A}^H(pk, ct^*, K^*)$	K* $\leftarrow_\$ \{0,1\}^{l_2}$
return b'	b' $\leftarrow_\$ \mathcal{A}^H(pk, ct^*, K^*)$
	return b'

Question 3. b) Let $\mathcal{A}$ be an adversary playing the KEM IND-CPA game let's prove the following Lemma :

$$\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathcal{A},\mathsf{KEM}} \leq \Pr[query] \tag{4}$$

To prove that, let's build an adversary $\mathcal{C}$ playing the game Γ^b :

Adversary: $\mathcal{C}(x, y)$
(pk, sk) $\leftarrow_\$ Gen(1^\lambda)$
ct$^* \leftarrow enc(pk, x)$
b' $\leftarrow_\$ \mathcal{A}^H(pk, ct^*, y)$
return b'

Through $\mathcal{C}$ we set $\mathcal{A}$ in the same settings as in the KEM IND-CPA game, so if $\mathcal{A}$ wins then $\mathcal{C}$ wins. Which implies :

$$\Pr[\Gamma^b(\mathcal{C}) \implies 1] = \Pr[\mathsf{IND\text{-}CPA}^b_{\mathsf{KEM}}(\mathcal{A}) \implies 1] \tag{5}$$

We note as well that the event *query* being "$\mathcal{A}$ queries x to H" is the same as the event $query_{\mathcal{C}}$ which is "$\mathcal{C}$ queries x to H". Using this fact, (5) and the result of **Question 2.** we can infer the following :

$$\begin{aligned}
\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathcal{A},\mathsf{KEM}} &= |\Pr[\mathsf{IND\text{-}CPA}^1_{\mathsf{KEM}}(\mathcal{A}) \implies 1] - \Pr[\mathsf{IND\text{-}CPA}^0_{\mathsf{KEM}}(\mathcal{A}) \implies 1]| \\
\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathcal{A},\mathsf{KEM}} &= |\Pr[\Gamma^0(\mathcal{C}) \implies 1] - \Pr[\Gamma^1(\mathcal{C}) \implies 1]| \\
\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathcal{A},\mathsf{KEM}} &\leq \Pr[query_{\mathcal{C}}] = \Pr[query]
\end{aligned}$$

Which proves the lemma. Now let H' be :

Oracle: $\mathsf{H}'(x)$
// before first query
`transcript` $\leftarrow ()$
// on a query
if $x = \perp$ **then**
| return `transcript`
end
y $\leftarrow H(x)$
`transcript` $\leftarrow x$
return y

Obviously, giving H or H' to $\mathcal{A}$ won't change its result because it behaves exactly as H except for a special symbol that $\mathcal{A}$ is not asking to the oracle. At last let's build $\mathcal{B}$ playing the OW-CPA game :

ok but won't work if enc is randomized. enc(pk, m*) is not necessarily equal to ct*
-1pt

Adversary: $\mathcal{B}(pk, ct^*)$
$\mathrm{K}^* \leftarrow_\$ \{0,1\}^{l_2}$
$\mathcal{A}^{H'}(pk, ct^*, K^*)$
$\mathtt{transcript} \leftarrow H'(\perp)$
for $x \in \mathit{transcript}$ **do**
  if $enc(pk, x) = ct^*$ **then**
    return x
  end
end
return $\perp$

If $query$ happens $\mathcal{B}$ wins because the plaintext will be in the transcript, which implies :

$$\Pr[query] \leq \mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathcal{B},\mathsf{PKC}}$$

So, using the lemma (4) :

$$\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathcal{A},\mathsf{KEM}} \leq \mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathcal{B},\mathsf{PKC}}$$

Therefor, if the PKC is OW-CPA then the KEM is IND-CPA.

2 Relations between primitives

Question 1.

$\mathsf{Gen}(1^\lambda)$:	$\mathsf{Encaps}(pk)$:	$\mathsf{Decaps}(sk, ct)$:
(sk, pk) $\leftarrow_\$ A(1^\lambda)$	(K, ct) $\leftarrow_\$ B(pk)$	K' $\leftarrow A(sk, ct)$
return *(pk, sk)*	**return** *(ct, K)*	**return** *K'*

We have $K = K_B$ and $K_A = K'$, so if the KA is correct, $K_A = K_B$, $K = K'$ and the KEM is correct.

Question 2. Let $\mathcal{A}$ be an adversary playing the KEM IND-CPA game and let's build $\mathcal{B}$ playing the key distinguisher game Γ_b :

Adversary: $\mathcal{B}(\mathtt{transcript}, K)$
b' $\leftarrow_\$ \mathcal{A}(\mathtt{transcript}[0], \mathtt{transcript}[1], K)$
return *b'*

In the Γ_b game $\texttt{transcript} = (m_a, m_b) = (pk, ct)$ so if $\mathcal{A}$ wins, $\mathcal{B}$ wins. If KA is secure against key distinguisher in a passive setting, then the KEM is IND-CPA.

Question 3. Gen is exactly the same.

enc(pk, pt) :	dec(sk, ct = (aux, ct)) :
(aux, K) $\leftarrow_\$$ Encaps(pk)	K $\leftarrow$ Decaps(sk, aux)
ct $\leftarrow$ Enc(K, pt)	pt $\leftarrow$ Dec(K, ct)
return *(aux, ct)*	**return** pt

We will now prove the correctness of our PKC which uses KEM and a symmetric blokc cipher by expanding the classical correctness game of a PKC :

CORR_{PKC} :
(sk, pk) $\leftarrow_\$$ $Gen(1^\lambda)$
(aux, K) $\leftarrow_\$$ $Encaps(pk)$
ct $\leftarrow$ $Enc(K, pt)$
K $\leftarrow$ $Decaps(sk, aux)$
pt' $\leftarrow$ $Dec(K, ct)$
return $1_{pt=pt'}$

So PKC is correct if $\Pr[\text{CORR}_{PKC} \Rightarrow \textbf{true}] = 1$, Where CORR is the above game. Here we supposed that the KEM and the block cipher are correct then Decaps(sk, Encaps(pk)[0]) = Encaps$[1] = K$ since it is the definition of KEM.

Question 4. Let $(\mathcal{A}_1, \mathcal{A}_2)$ be an adversary playing the PKC IND-CPA game and let's suppose that the KEM is IND-CPA and the block cipher is OT-CPA. We will build sequence of indistinguishable games to proove that the PKC is IND-CPA. First let's recap the PKC IND-CPA explicitly shown for our case :

Game: $\Gamma_b(\mathcal{A}_1, \mathcal{A}_2)$
(pk, sk) $\leftarrow_\$$ $Gen(1^\lambda)$
$(\text{pt}_0, pt_1, st) \leftarrow_\$ \mathcal{A}_1^H(pk)$
if $\|pt_0\| \neq \|pt_1\|$ **then**
  return *0*
end
(aux, K) $\leftarrow_\$$ *Encaps*(pk)
ct $\leftarrow$ *Enc*(K, pt_b)
b' $\leftarrow_\$ \mathcal{A}_2^H(st, (aux, ct))$
return b'

The KEM is IND-CPA so K looks random to any adversary. So we can change K with a truly random string to build the game Γ'_b which is indistinguishable from Γ_b :

Game: $\Gamma'_b(\mathcal{A}_1, \mathcal{A}_2)$
(pk, sk) $\leftarrow_\$$ $Gen(1^\lambda)$
$(\text{pt}_0, pt_1, st) \leftarrow_\$ \mathcal{A}_1^H(pk)$
if $\|pt_0\| \neq \|pt_1\|$ **then**
| **return** *0*
end
(aux, K) $\leftarrow_\$$ $\mathsf{Encaps}(pk)$
$K^* \leftarrow_\$ \{0,1\}^{l_2}$
$ct \leftarrow \mathsf{Enc}(K^*, pt_b)$
$b' \leftarrow_\$ \mathcal{A}_2^H(st, (aux, ct))$
return b'

Now we have the settings required to apply the OT-CPA property of the block cipher to change $\mathsf{Enc}(K, pt_b)$ to $\mathsf{Enc}(K, pt_0)$ to build the game Γ''_b which is indistinguishable from Γ'_b :

Game: $\Gamma''_b(\mathcal{A}_1, \mathcal{A}_2)$
(pk, sk) $\leftarrow_\$$ $Gen(1^\lambda)$
$(\text{pt}_0, pt_1, st) \leftarrow_\$ \mathcal{A}_1^H(pk)$
if $\|pt_0\| \neq \|pt_1\|$ **then**
| **return** *0*
end
(aux, K) $\leftarrow_\$$ $\mathsf{Encaps}(pk)$
$K^* \leftarrow_\$ \{0,1\}^{l_2}$
$ct \leftarrow \mathsf{Enc}(K^*, pt_0)$
$b' \leftarrow_\$ \mathcal{A}_2^H(st, (aux, ct))$
return b'

Now we have $\Gamma''_0 = \Gamma''_1$ so :

$$\Pr[\Gamma''_0(\mathcal{A}_1, \mathcal{A}_2) \implies 1] = \Pr[\Gamma''_1(\mathcal{A}_1, \mathcal{A}_2) \implies 1]$$
$$\mathsf{Adv}^{\Gamma''_b}_{\mathcal{A}_1,\mathcal{A}_2} = 0$$

Since Γ''_b and Γ_b are indistinguishable, the advantage of $(\mathcal{A}_1, \mathcal{A}_2)$ playing the Γ_b is negligible so the PKC is IND-CPA.

No clear bound and no explicit reductions -1pt