# Chapter 03

Mingjia Huo

**Problem 3.4.** *Proof.*

$$
\begin{aligned}
&\Pr[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\pi}(n)=1]\\
=&\Pr[b=0]\Pr[\mathrm{out}(\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n,0))=0]+\Pr[b=1]\Pr[\mathrm{out}(\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n,1))=1]\\
=&\Pr[b=0](1-\Pr[\mathrm{out}(\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n,0))=1])+\Pr[b=1]\Pr[\mathrm{out}(\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n,1))=1]\\
=&\frac{1}{2}(\Pr[\mathrm{out}(\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n,1))=1]-\Pr[\mathrm{out}(\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n,0))=1]+1)
\end{aligned}
$$

By DEFINITION 3.8, we have

$$\Pr[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n)=1]\leq\frac{1}{2}+\mathrm{negl}(n).$$

Additionally, if we have an adversary $\mathcal{A}$ such that $\Pr[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n)=1]<\frac{1}{2}-\mathrm{negl}(n)$, by simply inverse the $b'$ $\mathcal{A}$ outputs, we get $\Pr[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n)=1]>\frac{1}{2}+\mathrm{negl}(n)$, a contradiction. Thus, DEFINITION 3.8 implies

$$\Pr[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n)=1]\geq\frac{1}{2}-\mathrm{negl}(n).$$

So

$$
\begin{aligned}
&\text{DEFINITION 3.8}\\
\Leftrightarrow&\left|\Pr[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n)=1]-\frac{1}{2}\right|\leq\mathrm{negl}(n)\\
\Leftrightarrow&\left|\frac{1}{2}\left(\Pr[\mathrm{out}(\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n,1))=1]-\Pr[\mathrm{out}(\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n,0))=1]+1\right)-\frac{1}{2}\right|\leq\mathrm{negl}(n)\\
\Leftrightarrow&\left|\Pr[\mathrm{out}(\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n,1))=1]-\Pr[\mathrm{out}(\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n,0))=1]\right|\leq\mathrm{negl}(n)\\
\Leftrightarrow&\text{DEFINITION 3.9,}
\end{aligned}
$$

which finish the proof. □

**Problem 3.6. (a). Refute** when $n$ is odd:

If $|s|=n=2k+1$ and $l(n)=2n+1$, the length of the output of $G'(s)$ is $l(\lfloor\frac{n}{2}\rfloor)=2k+1=|s|$, which contradicts the condition that a pseudorandom generator satisfies $l(n)>n$.

**Prove** when $n$ is even:

By the definition of pseudorandomness, we have: For any PPT algorithm D, there is a negligible function negl such that

$$| \Pr[D(G(s)) = 1] - \Pr[D(r) = 1] | \leq \text{negl}(n),$$

where $s \in \{0,1\}^n, r \in \{0,1\}^{l(n)}$ are drawn uniformly.

So the claim is the same when $s^* \in \{0,1\}^{\lfloor n/2 \rfloor}, r^* \in \{0,1\}^{l(\lfloor n/2 \rfloor)}$.

And $G'(s) = G(s_1 \cdots s_{\lfloor n/2 \rfloor})$, where $s = s_1 \cdots s_n$. The length of the output of $G'(s)$ is $l(\lfloor n/2 \rfloor) = |r^*|$. So

$$\begin{aligned} & | \Pr[D(G'(s)) = 1] - \Pr[D(r^*) = 1] | \\ = & | \Pr[D(G(s^*)) = 1] - \Pr[D(r^*) = 1] | \\ \leq & \text{negl}(\lfloor n/2 \rfloor) \\ = & \text{negl}(n). \end{aligned}$$

So $G'(s)$ is a pseudorandom generator.

**(b). Refute**:

Using the conclusion in **(a)**: $G'(s) = G(s_1 \cdots s_{\lfloor n/2 \rfloor})$ is a pseudorandom generator, where $s = s_1 \cdots s_n$.

Prove by **Contradiction**: Assume $G(0^{|s|} \| s)$ is a pseudorandom generator. Then Use the conclusion in **(a)**, we have $G'(s) = G(0^{|s|})$ also a pseudorandom generator. However, $G(0^{|s|})$ can be easily distinguished from uniform strings.

Specifically, just let adversary $D$ compare its input with a fixed number $G(0^{n_0})$(Here $n_0$ is a fixed number.) Output 1 *if and only if* they are equal.

Uniformly choose $s_0 \in \{0,1\}^{n_0}$, we have

$$\Pr[D(G'(s_0)) = 1] = \Pr[D(G(0^{|s_0|}) = 1] = \Pr[D(G(0^{n_0})) = 1] = 1.$$

But randomly select $r_0 \in \{0,1\}^{l(n_0)}$, we have $r_0 = G(0^{n_0})$ with probability $2^{-l(n_0)}$. So

$$| \Pr[D(G'(s_0)) = 1] - \Pr[D(r_0) = 1] | = 1 - 2^{-l(n_0)} > \text{negl}(n_0),$$

a contradiction.

Thus $G(0^{|s|} \| s)$ is not a pseudorandom generator.

**(c). Refute**:

Prove by **Contradiction**: Assume $G(s)$ is a pseudorandom generator. Using the conclusion in **(a)**, we have $G''(s) = G(s_1 \cdots s_{\lfloor n/2 \rfloor})$ also a pseudorandom generator. However, $G'(s) = G''(s) \| G''(s+1)$ can be easily distinguished from uniform strings.

Construct $D$: it outputs 1 *if and only if* the first and second half of the input string is equal.

- If the input is $G'(s)$, we have $G'(s) = G''(s) \| G''(s+1)$. However, $G''(s) = G''(s+1)$ when the last $\lceil n/2 \rceil$ bits of $s$ is not $11 \cdots 1$, so the probability is $1 - 2^{\lceil n/2 \rceil}$. That is

$$\Pr[D(G''(s)) = 1] = 1 - 2^{\lceil n/2 \rceil}.$$

- If the input is $r \in \{0,1\}^{2l(\lfloor n/2 \rfloor)}$, we have

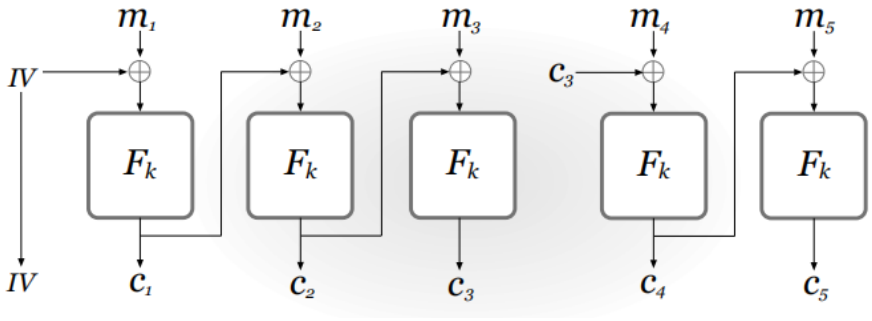
$$\Pr[D(r)=1] = \Pr[r_0 \cdots r_{l(\lfloor n/2 \rfloor)} = r_{l(\lfloor n/2 \rfloor)+1} \cdots r_{2l(\lfloor n/2 \rfloor)}] = 2^{\lfloor n/2 \rfloor} < \text{negl}(n).$$

- So

$$|\Pr[D(G''(s))=1] - \Pr[D(r)=1]| > 1 - 2^{\lceil n/2 \rceil} - \text{negl}(n) > \text{negl}(n),$$

a contradiction.

**Problem 3.11.** Construct a encryption theme like this:




In this picture, the last block of the previous ciphertext is used as the $IV$ when encrypting the next message.

**First**, it has indistinguishable multiple encryptions in the presence of an eavesdropper.

Given any adversary $\mathcal{A}$, we can construct a distinguisher $D$ which access an oracle $\mathcal{O}$:$\{0,1\}^n \to \{0,1\}^n$. In detail:

1. Run $\mathcal{A}(1^n)$. When $\mathcal{A}$ outputs $(m_1^0, \cdots, m_d^0)$ and $(m_1^1, \cdots, m_d^1)$, choose a uniform bit $b \in \{0,1\}$ and then:
   (a) Get the last ciphertext $c_0$ in the previous encryption(If this is the first encryption, randomly choose $c_0 = IV \in \{0,1\}^n$ with uniform distribution.)
   (b) Query $\mathcal{O}(c_0 \oplus m_1)$ and obtain response $c_1$, then Query $\mathcal{O}(c_1 \oplus m_2)$ and obtain response $c_2$,
   $\cdots$
   until it gets $(c_1, \cdots, c_d)$.
   (c) Return $(c_0, c_1, \cdots, c_d)$ to $\mathcal{A}$.
2. A outputs a bit $b'$. Output 1 if $b' = b$, and 0 otherwise.

Thus, $D$ outputs 1 *if and only if* $\mathcal{A}$ succeeds. Let $\Pi$ denotes our construction, and $\widetilde{\Pi}$ denotes the theme when we replace $F_k$ with a truly random function $f$. Then:

$$\Pr[\text{PrivK}^{mult}_{\mathcal{A},\Pi}(n)=1] = \Pr_{k \leftarrow \{0,1\}^n}[D^{F_k(\cdot)}(1^n)=1],$$

$$\Pr[\text{PrivK}^{mult}_{\mathcal{A},\widetilde{\Pi}}(n)=1] = \Pr_{f \leftarrow \text{Func}_n}[D^{f(\cdot)}(1^n)=1].$$

By the definition of pseudorandom function, we have

$$| \Pr[D^{F_k(\cdot)}(1^n) = 1] - \Pr[D^{f(\cdot)}(1^n) = 1] | \leq \text{negl}(n).$$

Thus

$$| \Pr[\text{PrivK}^{mult}_{\mathcal{A},\Pi}(n) = 1] - \Pr[\text{PrivK}^{mult}_{\mathcal{A},\widetilde{\Pi}}(n) = 1] | \leq \text{negl}(n).$$

To prove $\Pr[\text{PrivK}^{mult}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \text{negl}(n)$, we only need to prove:

$$\Pr[\text{PrivK}^{mult}_{\mathcal{A},\widetilde{\Pi}}(n) = 1] \leq \frac{1}{2} + \text{negl}(n)$$

We should know that $\text{Enc}_{c_0}(m_1, \cdots, m_d) = f(m_1 \oplus c_0, m_2 \oplus c_1, \cdots, m_d \oplus c_{d-1}) = f(m'_1, \cdots, m'_d) = (c_1, \cdots, c_d)$. Since $f$ is a random function, given $c \in \{0,1\}^n$, the probability of $f(\cdot) = c$ is $2^{-n}$. ($f$ is uniformly drawn from the set of all functions of $\{0,1\}^n \to \{0,1\}^n$.)

Define event Repeat which denotes that there exits $i \neq j \in \{1, 2 \cdots, n\}$ such that $c_i \oplus m_{i+1} = c_j \oplus m_{j+1}$. If there is no Repeat, then answer $(c_1, \cdots, c_d)$ is just a stream of uniform bits. So

$$\begin{aligned}
&\Pr[\text{PrivK}^{mult}_{\mathcal{A},\widetilde{\Pi}}(n) = 1] \\
=&\Pr[\text{PrivK}^{mult}_{\mathcal{A},\widetilde{\Pi}}(n) = 1 \wedge \text{Repeat}] + \Pr[\text{PrivK}^{mult}_{\mathcal{A},\widetilde{\Pi}}(n) = 1 \wedge \overline{\text{Repeat}}] \\
\leq&\frac{\mathcal{O}(d)}{2^n} + \frac{1}{2} \\
=&\frac{1}{2} + \text{negl}(n). \qquad (d \text{ is polynomial of n.})
\end{aligned}$$

Thus,

$$\Pr[\text{PrivK}^{mult}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \text{negl}(n).$$

which means the theme has indistinguishable multiple encryptions in the presence of an eavesdropper.

**Second**, it's not CPA-secure.
Construct an adversary $\mathcal{A}$:

1. $\mathcal{A}$ randomly select two different string $m_0, m_1 \in \{0,1\}^n$ and output them.
2. A uniform bit $b \in \{0,1\}$ is chosen, then a ciphertext $c = \text{Enc}_k(m_b) = (IV, c)$ is computed and given to $\mathcal{A}$.
3. $\mathcal{A}$ compute $m_2 = m_0 \oplus IV \oplus c$, and get access to $c_2 = \text{Enc}_k(m_2)$.
4. If $c = c_2$, $\mathcal{A}$ outputs 0; otherwise outputs 1.

When $b = 0$, then $m_0 \oplus IV = m_2 \oplus c$. Thus the input of $F_k$ is the same, and $c = c_2$ with probability 1. When $b = 1$, $c \neq c_2$ with high probability$(1 - 2^{-|c|})$. So $\mathcal{A}$ succeeds with probability near 1, which indicates that this theme is not CPA-secure.

**Problem 3.18.** How to decrypt: Given $k \in \{0,1\}^n, c$, compute $m' = F_k^{-1}(c)$. Message $m$ is the second half of $m'$.

**PART 1**: CPA-secure

*Proof.* Without loss of generality, assume the permutation is fixed length Given any adversary $\mathcal{A}$, we can construct a distinguisher $D$ which access an oracle $\mathcal{O}$:$\{0,1\}^n \to \{0,1\}^n$. In detail:

1. Run $\mathcal{A}(1^{2n})$. When $\mathcal{A}$ queries its encryption oracle on a message $m \in \{0,1\}^n$, answer this query in the following way:
   (a) choose uniform $r \in \{0,1\}^n$.
   (b) Query $\mathcal{O}(r\|m)$ and obtain response $y$.
   (c) Return the ciphertext $y$ to $\mathcal{A}$.
2. When $\mathcal{A}$ outputs messages $m_0, m_1 \in \{0,1\}^n$, choose a uniform bit $b \in \{0,1\}$ and then:
   (a) choose uniform $r_0 \in \{0,1\}^n$.
   (b) Query $\mathcal{O}(r_0\|m_b)$ and obtain response $y$.
   (c) Return the ciphertext $y$ to $\mathcal{A}$.
3. Continue answering encryption-oracle queries of $\mathcal{A}$ as before until $\mathcal{A}$ outputs a bit $b'$. Output 1 if $b' = b$, and 0 outherwise.

Thus, $D$ outputs 1 *if and only if* $\mathcal{A}$ succeeds. Let $\Pi$ denotes our construction, and $\widetilde{\Pi}$ denotes the theme when we replace $F_k$ with a uniform permutation $f \in \mathrm{Perm}_n$. Then:

$$\Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A},\Pi}(2n) = 1] = \Pr_{k \leftarrow \{0,1\}^{2n}}[D^{F_k(\cdot)}(1^{2n}) = 1],$$

$$\Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A},\widetilde{\Pi}}(2n) = 1] = \Pr_{f \leftarrow \mathrm{Perm}_{2n}}[D^{f(\cdot)}(1^{2n}) = 1].$$

By the definition of pseudorandom permutation, we have

$$|\Pr[D^{F_k(\cdot)}(1^{2n}) = 1] - \Pr[D^{f(\cdot)}(1^{2n}) = 1]| \leq \mathrm{negl}(2n).$$

Thus

$$|\Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A},\Pi}(2n) = 1] - \Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A},\widetilde{\Pi}}(2n) = 1]| \leq \mathrm{negl}(2n),$$

that is

$$|\Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A},\Pi}(n) = 1] - \Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A},\widetilde{\Pi}}(n) = 1]| \leq \mathrm{negl}(n).$$

To prove $\Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathrm{negl}(n)$, we only need to prove:

$$\Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A},\widetilde{\Pi}}(n) = 1] \leq \frac{1}{2} + \mathrm{negl}(n)$$

Define event Repeat which denotes $r_0$ was selected in some query. (There are totally $d = q(n)$ queries.) If there is no Repeat, then answer $c$ is just uniform bits. So

$$\begin{aligned}&\Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A},\widetilde{\Pi}}(n) = 1]\\ =&\Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A},\widetilde{\Pi}}(n) = 1 \wedge \mathrm{Repeat}] + \Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A},\widetilde{\Pi}}(n) = 1 \wedge \overline{\mathrm{Repeat}}]\end{aligned}$$

Separately,

1. $\Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A},\widetilde{\Pi}}(n) = 1 \wedge \mathrm{Repeat}]$:

   Since $r$ is drawn uniformly, the above probability is $\frac{\mathcal{O}(d)}{2^n} = \mathrm{negl}(n)$.

2. Let $R_{asked}$ denote the set of $r$ used by the experiment during the queries. And $R$ denotes the event that which $r$ is chosen.

$$\begin{aligned}&\Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A},\widetilde{\Pi}}(n) = 1 \wedge \overline{\mathrm{Repeat}}]\\ =&\Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A},\widetilde{\Pi}}(n) = 1 \mid \overline{\mathrm{Repeat}}] \times \Pr[\overline{\mathrm{Repeat}}]\\ =&\Pr[\overline{\mathrm{Repeat}}] \sum_{r \notin R_{asked}} \Pr[R = r](\Pr[\mathrm{Enc}(r\|m_0) = c]\Pr[b = 0] + \Pr[\mathrm{Enc}(r\|m_1) = c]\Pr[b = 1])\\ =&\Pr[\overline{\mathrm{Repeat}}] \sum_{r \notin R_{asked}} \Pr[R = r](\Pr[\mathrm{Enc}(r\|m_1) = c]\Pr[b = 0] + \Pr[\mathrm{Enc}(r\|m_0) = c]\Pr[b = 1])\\ =&\Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A},\widetilde{\Pi}}(n) = 0 \wedge \overline{\mathrm{Repeat}}]\end{aligned}$$

   So

$$\Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A},\widetilde{\Pi}}(n) = 1 \wedge \overline{\mathrm{Repeat}}] = \frac{1}{2}$$

Thus,

$$\begin{aligned}&\Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A},\widetilde{\Pi}}(n) = 1]\\ =&\Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A},\widetilde{\Pi}}(n) = 1 \wedge \mathrm{Repeat}] + \Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A},\widetilde{\Pi}}(n) = 1 \wedge \overline{\mathrm{Repeat}}]\\ \leq&\frac{1}{2} + \mathrm{negl}(n)\end{aligned}$$

which means CPA-secure.

□

**PART 2**: The proof of CCA-secure is the same with problem 4.25.

**Problem 3.29.** Define when given $1^n$ to Gen, the message is $l_{in}(n)$ in length, which is polynomial in $n$. For that reason, we can assume $l_{in}(n) = n$, which don't affect the result of $\mathrm{negl}(n)$. Construct a theme $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ as followed:

1. Gen: on input $1^n$, choose $(k_1, k_2)$ based on the $\mathrm{Gen}_1(1^n), \mathrm{Gen}_2(1^n)$ in $\Pi_1, \Pi_2$.

2. Enc: Given $m \in \{0,1\}^n$, uniformly select a $m_l \in \{0,1\}^n$. Then compute $m_r = m \oplus m_l$. Use $\mathrm{Enc}_1^{k_1}$ to encrypt $m_l$ and $\mathrm{Enc}_2^{k_2}$ to encrypt $m_r$. The ciphertext we get is $(c_1, c_2)$.

3. Dec: $m = \mathrm{Dec}_1^{k_1}(c_1) \oplus \mathrm{Dec}_2^{k_2}(c_2)$.

*Proof.* Now we prove it's CPA-secure.

Assume there is an adversary $\mathcal{A}$ for $\Pi$. Construct an adversary $\mathcal{A}_2$ for $\Pi$ as followed:

1. $\mathcal{A}_2$ has oracle $\mathrm{Enc}_{k_2}(\cdot)$, with $k_2$ unknown to $\mathcal{A}_2$. But $\mathcal{A}_2$ can choose $k_1 \leftarrow \mathrm{Gen}_1(1^n)$, then construct a new oracle

$$\mathrm{Enc}_{k_1,k_2}(\cdot) = (\mathrm{Enc}_{k_1}(m_l), \mathrm{Enc}_{k_2}(m_l \oplus \cdot)).$$

   Here $m_l \in \{0,1\}^n$ is uniformly selected by the oracle.

2. $\mathcal{A}$ queries the oracle $\mathrm{Enc}_{k_1,k_2}(\cdot)$ and get the ciphertexts.

3. $\mathcal{A}$ asks $m_0', m_1'$. Then $\mathcal{A}_2$ uniformly choose $m_l \in \{0,1\}^n$, construct $(m_0, m_1) = (m_l \oplus m_0', m_l \oplus m_1')$ and ask the CPA-experiment. Then $\mathcal{A}_2$ get $c$, and pass $(\mathrm{Enc}_{k_1}(m_l), c)$ to $\mathcal{A}$.

4. $\mathcal{A}$ asks some queries to $\mathrm{Enc}_{k_1,k_2}(\cdot)$ and output $b' \in \{0,1\}$.

5. $\mathcal{A}_2$ output $b'$.

In this experiment, both $\mathcal{A}$ and $\mathcal{A}_2$ don't know $b$, and what $\mathcal{A}_2$ guesses is the same as what $\mathcal{A}$ guesses. Also,

$$\begin{aligned}
&\mathrm{PrivK}^{cpa}_{\mathcal{A}_2,\Pi}(n) = 1 \\
\Leftrightarrow &c = \mathrm{Enc}_{k_2}(m_{b'}) \\
\Leftrightarrow &(\mathrm{Enc}_{k_1}(m_l), c) = (\mathrm{Enc}_{k_1}(m_l), \mathrm{Enc}_{k_2}(m_l \oplus m_{b'}')) \\
\Leftrightarrow &\mathrm{PrivK}^{cpa}_{\mathcal{A},\Pi}(n) = 1.
\end{aligned}$$

So

$$\Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A}_2,\Pi}(n) = 1] = \Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A},\Pi}(n) = 1].$$

Similarly, we can construct an adversary $\mathcal{A}_1$ such that

$$\Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A}_1,\Pi}(n) = 1] = \Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A},\Pi}(n) = 1].$$

So if $\Pi$ is not CPA-secure, then $\exists \mathcal{A}, s.t. \Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A},\Pi}(n) = 1] > \frac{1}{2} + \mathrm{negl}(n)$, so

$$\Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A}_2,\Pi}(n) = 1] = \Pr[\mathrm{PrivK}^{cpa}_{\mathcal{A}_1,\Pi}(n) = 1] > \frac{1}{2} + \mathrm{negl}(n),$$

which means that each of $\Pi_1$ and $\Pi_2$ is not CPA-secure, a contradiction.

Thus $\Pi$ is CPA-secure. □