

Midterm I

Name:

SID:

- Write your name and SID in the boxes above now. Do NOT open the exam until 12:40 PM. The exam runs from 12:40 PM to 2:00 PM.
- This exam has 5 questions (85 points total) and 19 pages (including this cover page). Notify a proctor immediately if a page is missing.
- You may consult at most *1 double-sided sheet of handwritten notes*. Apart from that, you may not look at books, notes, etc. Calculators, phones, computers, tablets, and all other electronic devices are NOT permitted.
- DSP Students: If you are allowed $1.5\times$ (resp. $2\times$) the regular exam duration, then you must submit your exam within $120 = 80 \times 1.5$ (resp. $160 = 80 \times 2$) mins.
- We will not be answering questions during the exam. If you feel that something is unclear please write a note in your answer.

1 Perfect Secrecy (15 points)

For a set S , let $s \xleftarrow{\$} S$ denote selecting a uniformly random element s from S .

Definition (Perfect Secrecy). An encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ with message space $\mathcal{M}$ is *perfectly secret* if for every adversary $\mathcal{A}$, $\Pr[\text{PrivK}_{\mathcal{A}, \Pi}^{\text{eav}} = 1] = \frac{1}{2}$, where the game is defined as follows.

Game $\text{PrivK}_{\mathcal{A}, \Pi}^{\text{eav}}$:

1. $\mathcal{A}$ outputs $m_0, m_1 \in \mathcal{M}$.
2. $b \xleftarrow{\$} \{0, 1\}$, $k \leftarrow \text{Gen}()$, $c \leftarrow \text{Enc}(k, m_b)$.
3. $\mathcal{A}$ is given the challenge ciphertext c .
4. $\mathcal{A}$ outputs b' .
5. The game outputs 1 if $b' = b$, and 0 otherwise.

Consider the following encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ for the message space $\{0, 1\}$.

- **Gen:** Choose three random bits $\alpha, \beta, \gamma \xleftarrow{\$} \{0, 1\}$. Output (α, β, γ) .
- **Enc** $((\alpha, \beta, \gamma), m)$: Choose random bits $x_1, x_2 \xleftarrow{\$} \{0, 1\}$ and compute x_3 such that $\alpha \cdot x_1^2 + \beta \cdot x_2 + x_3 + \gamma = m$ where $+$ and $\cdot$ are addition and multiplication of bits in $\{0, 1\}$, taken modulo 2 (so $1 + 1 = 0$). Output (x_1, x_2, x_3) .
- **Dec** $((\alpha, \beta, \gamma), (x_1, x_2, x_3))$: Output $m = \alpha \cdot x_1^2 + \beta \cdot x_2 + x_3 + \gamma$.

(a) **(8 points)** Show that this scheme is perfectly secret.

Solution: Since all arithmetic is over $\{0, 1\}$, we have $x_1^2 = x_1$. Fix any message $m \in \{0, 1\}$ and any ciphertext $c = (u, v, w) \in \{0, 1\}^3$. For an encryption of m to equal c , the encryption algorithm must first sample $x_1 = u$ and $x_2 = v$, which happens with probability $1/4$. It must then be the case that

$$\alpha u + \beta v + \gamma = m + w.$$

For each of the four choices of (α, β) , there is exactly one choice of γ satisfying this equation. Thus a uniformly random key satisfies the equation with probability $4/8 = 1/2$, and therefore

$$\Pr[\text{Enc}((\alpha, \beta, \gamma), m) = c] = \frac{1}{4} \cdot \frac{1}{2} = \frac{1}{8}.$$

This probability is the same for every m and every c . Consequently, the challenge ciphertext is uniform over $\{0, 1\}^3$ and independent of the challenge bit b . Every adversary therefore guesses b correctly with probability exactly $1/2$, so the scheme is perfectly secret.

Alternative solution: Let M and $C = (X_1, X_2, X_3)$ denote the message and ciphertext random variables. Fix any $m \in \{0, 1\}$ and any $c = (c_1, c_2, c_3) \in \{0, 1\}^3$. First,

$$\begin{aligned} \Pr[C = c \mid M = m] &= \Pr[X_1 = c_1, X_2 = c_2, X_3 = c_3 \mid M = m] \\ &= \Pr[X_1 = c_1, X_2 = c_2, \alpha X_1^2 + \beta X_2 + c_3 + \gamma = m \mid M = m] \\ &= \Pr[X_1 = c_1 \mid M = m] \\ &\quad \cdot \Pr[X_2 = c_2 \mid M = m, X_1 = c_1] \\ &\quad \cdot \Pr[\alpha c_1^2 + \beta c_2 + c_3 + \gamma = m \mid M = m, X_1 = c_1, X_2 = c_2]. \end{aligned}$$

For the final conditional probability, fix any values of α and β . The equation then determines exactly one value

$$\gamma = m + \alpha c_1^2 + \beta c_2 + c_3$$

of the uniform independent bit γ , so the probability is $1/2$ for every fixed (α, β) and remains $1/2$ after averaging over α and β . Therefore,

$$\begin{aligned} \Pr[C = c \mid M = m] &= \Pr[X_1 = c_1 \mid M = m] \cdot \Pr[X_2 = c_2 \mid M = m, X_1 = c_1] \\ &\quad \cdot \Pr[\alpha c_1^2 + \beta c_2 + c_3 + \gamma = m \mid M = m, X_1 = c_1, X_2 = c_2] \\ &= \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{8}. \end{aligned}$$

It follows that

$$\Pr[C = c] = \sum_{m' \in \{0, 1\}} \Pr[C = c \mid M = m'] \Pr[M = m'] = \frac{1}{8}.$$

Applying Bayes' rule gives

$$\Pr[M = m \mid C = c] = \frac{\Pr[C = c \mid M = m] \Pr[M = m]}{\Pr[C = c]} = \frac{(1/8) \Pr[M = m]}{1/8} = \Pr[M = m].$$

Thus the scheme is perfectly secret.

-
- (b) **(7 points)** Consider the following game, $\text{PrivK}_{\mathcal{A}, \Pi}^{\text{kpa}}$, which describes utilizing a known-plaintext attack to attempt to decrypt a second, unknown plaintext.

Game $\text{PrivK}_{\mathcal{A}, \Pi}^{\text{kpa}}$:

1. $m_1, m_2 \xleftarrow{\$} \{0, 1\}^*$, $(\alpha, \beta, \gamma) \leftarrow \text{Gen}()$,
 $c_1 \leftarrow \text{Enc}((\alpha, \beta, \gamma), m_1)$, $c_2 \leftarrow \text{Enc}((\alpha, \beta, \gamma), m_2)$.
2. $\mathcal{A}$ is given plaintext m_1 and ciphertexts c_1 and c_2 .
3. $\mathcal{A}$ outputs m'_2 .
4. The game outputs 1 if $m'_2 = m_2$, and 0 otherwise.

Describe an adversary $\mathcal{A}$ such that $\Pr[\text{PrivK}_{\mathcal{A}, \Pi}^{\text{kpa}} = 1] > 1/2$, and justify its success probability.

Hint: Notice that the known plaintext-ciphertext pair (m_1, c_1) reveals some information about the key. Is the full key always necessary to decrypt a ciphertext, or is partial key information sometimes enough?

Name:

Solution: Write $c_1 = (x_1, x_2, x_3)$ and $c_2 = (y_1, y_2, y_3)$. The adversary acts as follows:

(a) If $(x_1, x_2) = (y_1, y_2)$, output

$$m'_2 = m_1 + x_3 + y_3.$$

(b) Otherwise, output a uniformly random bit.

To see why the first case works, correctness of the two ciphertexts gives

$$m_1 = \alpha x_1 + \beta x_2 + x_3 + \gamma,$$

$$m_2 = \alpha y_1 + \beta y_2 + y_3 + \gamma.$$

When $(x_1, x_2) = (y_1, y_2)$, adding these equations modulo 2 cancels the terms involving the key, giving $m_2 = m_1 + x_3 + y_3$. Hence the adversary is correct with probability 1 in this case.

The pairs (x_1, x_2) and (y_1, y_2) are sampled independently and uniformly from $\{0, 1\}^2$, so they agree with probability $1/4$. If they do not agree, the adversary's independent random guess is correct with probability $1/2$. Therefore

$$\Pr[\text{PrivK}_{\mathcal{A}, \Pi}^{\text{kpa}} = 1] = \frac{1}{4} \cdot 1 + \frac{3}{4} \cdot \frac{1}{2} = \frac{5}{8} > \frac{1}{2}.$$

2 Pseudorandom Functions (15 points)

Definition (Pseudorandom Function). Let $F : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ be an efficient keyed function. F is a *pseudorandom function (PRF)* if for all PPT adversaries $\mathcal{A}$,

$$\Pr[\text{PRF}_{\mathcal{A}, F}(n) = 1] \leq \frac{1}{2} + \text{negl}(n),$$

where Func_n denotes the set of all functions from $\{0, 1\}^n$ to $\{0, 1\}^n$ and the game is defined as follows.

Game $\text{PRF}_{\mathcal{A}, F}(n)$:

1. $b \xleftarrow{\$} \{0, 1\}$.
2. If $b = 0$: $k \xleftarrow{\$} \{0, 1\}^n$ and set $\mathcal{O} := F(k, \cdot)$. If $b = 1$: $f \xleftarrow{\$} \text{Func}_n$ and set $\mathcal{O} := f(\cdot)$.
3. $\mathcal{A}$ is given 1^n and oracle access to $\mathcal{O}(\cdot)$: it may query any $x \in \{0, 1\}^n$ and receives $\mathcal{O}(x)$.
4. $\mathcal{A}$ outputs a guess b' .
5. The game outputs 1 if $b' = b$, and 0 otherwise.

Let $F : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ be a pseudorandom function, and let $G : \{0, 1\}^n \times (\{0, 1\}^n \times \{0, 1\}^n) \rightarrow \{0, 1\}^n$ be defined as follows: for key $k \in \{0, 1\}^n$ and input (x, y) with $x, y \in \{0, 1\}^n$,

$$G(k, (x, y)) = F(k, x) \oplus y$$

where $\oplus$ denotes bitwise XOR. *Prove that G is not a secure pseudorandom function.*

The definition of a PRF above applies to G , with inputs $(x, y) \in \{0, 1\}^n \times \{0, 1\}^n$ in place of $x \in \{0, 1\}^n$, and Func_n replaced by the set of all functions from $\{0, 1\}^n \times \{0, 1\}^n$ to $\{0, 1\}^n$.

The parts below will outline the proof that G is not pseudorandom and ask you to fill in the missing details to complete the proof.

To show that G is not a secure PRF, let us construct an adversary $\mathcal{A}$ that wins the game $\text{PRF}_{\mathcal{A}, G}(n)$ with probability noticeably greater than $\frac{1}{2}$.

1. **(2 points)** $\mathcal{A}$ makes two queries (x, y) and (x', y') to its oracle $\mathcal{O}$:

$(x, y) =$

$(x', y') =$

Solution: Choose any arbitrary (x, y) and set $x' = x$ and $y' = \neg y$ (flip all bits of y).

Let z and z' be the responses obtained.

Name:

2. (2 points) Next, $\mathcal{A}$ outputs $b' = 0$ if

and outputs $b' = 1$ otherwise.

Solution: $\mathcal{A}$ outputs $b' = 0$ if $z \oplus z' = 1^n$.

3. (3 points) *Pseudorandom case* ($b = 0$): In the case where $\mathcal{O} = G(k, \cdot)$, what is $\Pr[b' = 0 \mid b = 0]$? Here the probability is over the randomness of $\mathcal{A}$ and the randomness of sampling k . Explain your reasoning.

Solution: $\Pr[b' = 0 \mid b = 0] = 1$ because $G(k, (x, y)) \oplus G(k, (x, \neg y)) = F(k, x) \oplus y \oplus F(k, x) \oplus \neg y = y \oplus \neg y = 1^n$ with certainty.

4. (3 points) *Truly random case* ($b = 1$): Here $\mathcal{O} = f$, where f is sampled uniformly at random from the set of all functions from $\{0, 1\}^n \times \{0, 1\}^n$ to $\{0, 1\}^n$.

In this case, what is $\Pr[b' = 1 \mid b = 1]$? Here the probability is over the randomness of $\mathcal{A}$ and the randomness of sampling f .

Explain your reasoning.

Solution: For any given (x, y) and (x', y') with $(x, y) \neq (x', y')$, the value of $f(x, y) \oplus f(x, \neg y)$ is uniformly random over $\{0, 1\}^n$, where the randomness is over the choice of f . Therefore, $\mathcal{A}$ outputs $b' = 0$ with probability 2^{-n} , so $\Pr[b' = 1 \mid b = 1] = 1 - 2^{-n}$.

5. (5 points) Finish the proof by computing $\Pr[\text{PRF}_{\mathcal{A}, G}(n) = 1]$, to argue that $\mathcal{A}$ breaks PRF security for G .

Solution: Since b is uniform,

$$\Pr[\text{PRF}_{\mathcal{A},G}(n) = 1] = \frac{1}{2} \Pr[b' = 0 \mid b = 0] + \frac{1}{2} \Pr[b' = 1 \mid b = 1] = \frac{1}{2} \cdot 1 + \frac{1}{2} (1 - 2^{-n}) = 1 - 2^{-(n+1)}.$$

This exceeds $\frac{1}{2}$ by $\frac{1}{2} - 2^{-(n+1)} \geq \frac{1}{4}$, which is not negligible, and $\mathcal{A}$ is PPT (it makes two queries). Therefore, G is not a secure PRF.

Name:

3 Pseudorandom Functions Again (15 points)

Definition (Pseudorandom Function). Let $F : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ be an efficient keyed function. F is a *pseudorandom function (PRF)* if for all PPT adversaries $\mathcal{A}$,

$$\Pr[\text{PRF}_{\mathcal{A},F}(n) = 1] \leq \frac{1}{2} + \text{negl}(n),$$

where Func_n denotes the set of all functions from $\{0, 1\}^n$ to $\{0, 1\}^n$ and the game is defined as follows.

Game $\text{PRF}_{\mathcal{A},F}(n)$:

1. $b \xleftarrow{\$} \{0, 1\}$.
2. If $b = 0$: $k \xleftarrow{\$} \{0, 1\}^n$ and set $\mathcal{O} := F(k, \cdot)$. If $b = 1$: $f \xleftarrow{\$} \text{Func}_n$ and set $\mathcal{O} := f(\cdot)$.
3. $\mathcal{A}$ is given 1^n and oracle access to $\mathcal{O}(\cdot)$: it may query any $x \in \{0, 1\}^n$ and receives $\mathcal{O}(x)$.
4. $\mathcal{A}$ outputs a guess b' .
5. The game outputs 1 if $b' = b$, and 0 otherwise.

Let $F : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ be a pseudorandom function. Prove that the following function H is also a pseudorandom function:

$$H(k, x) = F(k, x) \oplus x$$

Question 3 (continued)

Name:

Solution:

1. We will prove that if there exists an adversary D_H that distinguishes $H(k, \cdot)$ from $R_1(\cdot)$ with non-negligible advantage, then we can construct an adversary D_F that distinguishes $F(k, \cdot)$ from $R_2(\cdot)$ with the same advantage.

Description of D_F :

- (a) D_F runs D_H .
 - (b) Whenever D_H outputs a query x , D_F forwards the query to its oracle to get a response y . Then it sends to D_H the response $y \oplus x$.
 - (c) Finally, D_F outputs whatever D_H outputs.
2. *Pseudorandom case:* If D_F is interacting with an oracle for $F(k, \cdot)$, then it has successfully simulated D_H 's interaction with an oracle for $H(k, \cdot)$.

$$\Pr[D_F^{F(k, \cdot)} = 1] = \Pr[D_H^{H(k, \cdot)} = 1]$$

3. *Truly random case:* Let us define

$$R_1(x) = R_2(x) \oplus x$$

If R_2 is a uniformly random function, then so is R_1 . Therefore, if D_F is interacting with an oracle for $R_2(\cdot)$, then it has successfully simulated D_H 's interaction with a different random function R_1 .

$$\Pr[D_F^{R_2(\cdot)} = 1] = \Pr[D_H^{R_1(\cdot)} = 1]$$

4. In summary:

$$\left| \Pr[D_F^{F(k, \cdot)} = 1] - \Pr[D_F^{R_2(\cdot)} = 1] \right| = \left| \Pr[D_H^{H(k, \cdot)} = 1] - \Pr[D_H^{R_1(\cdot)} = 1] \right|$$

5. Assume toward contradiction that H is not a PRF. Then there exists a D_H such that $\left| \Pr[D_H^{H(k, \cdot)} = 1] - \Pr[D_H^{R_1(\cdot)} = 1] \right|$ is non-negligible. Then we've shown that there exists a D_F such that $\left| \Pr[D_F^{F(k, \cdot)} = 1] - \Pr[D_F^{R_2(\cdot)} = 1] \right|$ is non-negligible. This implies that F is not a PRF, which is contradiction.
6. Therefore our assumption must be false, so in fact, H is a PRF.

4 Shrinking the Ciphertext (20 points)

Definition (CPA Security). An encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ is *CPA-secure* if for all PPT adversaries $\mathcal{A}$,

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

where the game is defined as follows.

Game $\text{PrivK}_{\mathcal{A}, \Pi}^{\text{CPA}}(n)$:

1. $k \leftarrow \text{Gen}(1^n)$. $\mathcal{A}$ is given 1^n and oracle access to $\text{Enc}(k, \cdot)$.
2. $\mathcal{A}^{\text{Enc}(k, \cdot)}$ outputs m_0, m_1 with $|m_0| = |m_1|$.
3. $b \xleftarrow{\$} \{0, 1\}$, $c^* \leftarrow \text{Enc}(k, m_b)$.
4. c^* is given to $\mathcal{A}^{\text{Enc}(k, \cdot)}$.
5. $\mathcal{A}^{\text{Enc}(k, \cdot)}$ outputs a guess b' .
6. The game outputs 1 if $b' = b$, and 0 otherwise.

Recall the CPA-secure encryption scheme from lecture: $\text{Enc}(k, m) = \langle r, F(k, r) \oplus m \rangle$ with $r \xleftarrow{\$} \{0, 1\}^n$. One downside of this scheme is that the ciphertext is twice as long as the message. To save bandwidth, an engineer proposes to use a *shorter* random string r .

Let $F : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ be a pseudorandom function, and let $\ell = \ell(n)$ be a function with $1 \leq \ell(n) \leq n$. Define the encryption scheme $\Pi_\ell = (\text{Gen}, \text{Enc}, \text{Dec})$ for messages $m \in \{0, 1\}^n$:

- $\text{Gen}(1^n)$: Output $k \xleftarrow{\$} \{0, 1\}^n$.
- $\text{Enc}(k, m)$: Sample $r \xleftarrow{\$} \{0, 1\}^\ell$ and output the ciphertext
$$c := \langle r, F(k, r \| 0^{n-\ell}) \oplus m \rangle.$$
- $\text{Dec}(k, \langle r, s \rangle)$: Output $F(k, r \| 0^{n-\ell}) \oplus s$.

The ciphertext now has length $n + \ell$ instead of $2n$. Throughout this question, $\log$ denotes $\log_2$.

Name:

- (a) **(8 points)** Let $\ell(n) = \lceil \log n \rceil$. Describe an adversary $\mathcal{A}$ that makes *exactly one* query to the encryption oracle and wins the game $\text{PrivK}_{\mathcal{A}, \Pi_\ell}^{\text{CPA}}(n)$ with probability at least $\frac{1}{2} + \frac{1}{4n}$. Justify this success probability, and explain why it shows that Π_ℓ is not CPA-secure.

Solution:

- Adversary $\mathcal{A}$:

- (a) Fix any two distinct messages, e.g. $m_0 = 0^n$ and $m_1 = 1^n$.
- (b) Query the encryption oracle on m_0 and receive $\langle r_1, s_1 \rangle$.
- (c) Submit (m_0, m_1) as the challenge and receive $c^* = \langle r^*, s^* \rangle$.
- (d) If $r^* = r_1$: output 0 if $s^* = s_1$ and output 1 otherwise. If $r^* \neq r_1$: output a uniformly random bit.

- Analysis: If $r^* = r_1$, then $s_1 = F(k, r_1 \| 0^{n-\ell}) \oplus m_0$ and $s^* = F(k, r_1 \| 0^{n-\ell}) \oplus m_b$, so $s^* = s_1$ if and only if $m_b = m_0$, i.e. if and only if $b = 0$ (since $m_0 \neq m_1$). So in this case $\mathcal{A}$ is always correct. Otherwise, $\mathcal{A}$ is correct with probability $\frac{1}{2}$.

Since r^* is uniform over $\{0, 1\}^\ell$ and independent of r_1 , $\Pr[r^* = r_1] = 2^{-\ell}$. Since $\ell = \lceil \log n \rceil < \log n + 1$, we have $2^\ell < 2n$, so $2^{-\ell} > \frac{1}{2n}$. Therefore

$$\Pr[\mathcal{A} \text{ wins}] = 2^{-\ell} \cdot 1 + (1 - 2^{-\ell}) \cdot \frac{1}{2} = \frac{1}{2} + \frac{2^{-\ell}}{2} > \frac{1}{2} + \frac{1}{4n}.$$

- $\mathcal{A}$ is PPT, and its advantage $\frac{1}{4n}$ is an inverse polynomial, hence non-negligible. So Π_ℓ is not CPA-secure.
- Intuition: The proof from lecture relies on r^* being “fresh.” With only $2^\ell \approx n$ possible values of r , a repeat happens with noticeable probability, and a repeated r means a repeated one-time pad.

- (b) **(12 points)** Prove that for $\ell(n) = \lceil (\log n)^2 \rceil$ (assume n is large enough that $\ell(n) \leq n$), the scheme Π_ℓ is CPA-secure. You may follow the structure of the proof from lecture, but be explicit about where the choice of ℓ is used.

Name:

Question 4(b) (continued)

Solution:

1. Assume toward contradiction that there is a PPT adversary $\mathcal{A}$ that makes at most $q(n)$ encryption queries (for some polynomial q) and wins the CPA security game for Π_ℓ with probability $\frac{1}{2} + \epsilon(n)$, for non-negligible ϵ . We construct a distinguisher $\mathcal{B}$ that breaks the PRF security of F .
2. Description of $\mathcal{B}^{\mathcal{O}(\cdot)}$, where $\mathcal{O}$ is either $F(k, \cdot)$ for uniform k , or a truly random function f :
 - (a) $\mathcal{B}$ runs $\mathcal{A}(1^n)$ and plays the role of the CPA challenger.
 - (b) When $\mathcal{A}$ queries its encryption oracle on m : $\mathcal{B}$ samples $r \xleftarrow{\$} \{0, 1\}^\ell$, queries $\mathcal{O}(r \| 0^{n-\ell})$, and returns $\langle r, \mathcal{O}(r \| 0^{n-\ell}) \oplus m \rangle$.
 - (c) When $\mathcal{A}$ outputs challenge messages (m_0, m_1) : $\mathcal{B}$ samples $b \xleftarrow{\$} \{0, 1\}$ and $r^* \xleftarrow{\$} \{0, 1\}^\ell$, queries $\mathcal{O}(r^* \| 0^{n-\ell})$, and returns $c^* = \langle r^*, \mathcal{O}(r^* \| 0^{n-\ell}) \oplus m_b \rangle$.
 - (d) When $\mathcal{A}$ outputs b' : $\mathcal{B}$ outputs 1 if $b' = b$, and 0 otherwise.

$\mathcal{B}$ is PPT since $\mathcal{A}$ is PPT.

3. *Pseudorandom case*: If $\mathcal{O} = F(k, \cdot)$, then every ciphertext $\mathcal{B}$ gives to $\mathcal{A}$ is distributed exactly as in Π_ℓ , so $\mathcal{A}$'s view is exactly the CPA security game for Π_ℓ . Hence

$$\Pr[\mathcal{B}^{F(k, \cdot)} = 1] = \Pr[\mathcal{A} \text{ wins}] = \frac{1}{2} + \epsilon(n).$$

4. *Truly random case*: Suppose $\mathcal{O} = f$. Let $r_1, \dots, r_q$ be the random strings used to answer $\mathcal{A}$'s encryption queries, and let Coll be the event that $r^* = r_i$ for some i .
 - If Coll does not happen, then $r^* \| 0^{n-\ell}$ differs from every $r_i \| 0^{n-\ell}$ (distinct r 's give distinct inputs to f), so $f(r^* \| 0^{n-\ell})$ is uniform and independent of everything else $\mathcal{A}$ sees. Then c^* is a one-time pad encryption of m_b , and $\mathcal{A}$ guesses b with probability exactly $\frac{1}{2}$.
 - Since r^* is uniform in $\{0, 1\}^\ell$ and independent of the r_i 's, a union bound gives $\Pr[\text{Coll}] \leq \frac{q(n)}{2^{\ell(n)}}$.

Therefore

$$\Pr[\mathcal{B}^{f(\cdot)} = 1] = \Pr[b' = b] \leq \frac{1}{2} + \Pr[\text{Coll}] \leq \frac{1}{2} + \frac{q(n)}{2^{\ell(n)}}.$$

5. *Where the choice of ℓ is used*: With $\ell(n) = \lceil (\log n)^2 \rceil$,

$$\frac{q(n)}{2^{\ell(n)}} \leq \frac{q(n)}{2^{(\log n)^2}} = \frac{q(n)}{n^{\log n}},$$

which is negligible, because $2^{-(\log n)^2}$ is negligible and a polynomial times a negligible function is negligible. (For $\ell(n) = \lceil \log n \rceil$ this term would be about $q(n)/n$, which is *not* negligible. That is exactly why the proof breaks down in part (a).)

6. *Putting it together*:

$$\left| \Pr[\mathcal{B}^{F(k, \cdot)} = 1] - \Pr[\mathcal{B}^{f(\cdot)} = 1] \right| \geq \epsilon(n) - \frac{q(n)}{2^{\ell(n)}}.$$

A non-negligible function minus a negligible function is non-negligible, so $\mathcal{B}$ breaks the PRF security of F . This is a contradiction, so Π_ℓ is CPA-secure.

Name:

5 CCA-Secure Encryption (20 points)

Definition (CCA Security). An encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ is *CCA-secure* if for all PPT adversaries $\mathcal{A}$,

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

where the game is defined as follows.

Game $\text{PrivK}_{\mathcal{A}, \Pi}^{\text{CCA}}(n)$:

1. $k \leftarrow \text{Gen}(1^n)$. $\mathcal{A}$ is given 1^n and oracle access to $\text{Enc}(k, \cdot)$ and $\text{Dec}(k, \cdot)$.
2. $\mathcal{A}^{\text{Enc}(k, \cdot), \text{Dec}(k, \cdot)}$ outputs m_0, m_1 with $|m_0| = |m_1|$.
3. $b \xleftarrow{\$} \{0, 1\}$, $c^* \leftarrow \text{Enc}(k, m_b)$.
4. c^* is given to $\mathcal{A}^{\text{Enc}(k, \cdot), \text{Dec}(k, \cdot)}$, which may *not* query $\text{Dec}(k, \cdot)$ on c^* .
5. $\mathcal{A}^{\text{Enc}(k, \cdot), \text{Dec}(k, \cdot)}$ outputs a guess b' .
6. The game outputs 1 if $b' = b$, and 0 otherwise.

Let $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ be a CCA-secure encryption scheme, and assume its ciphertexts are in $\{0, 1\}^n$. Consider the following encryption scheme $\Pi' = (\text{Gen}', \text{Enc}', \text{Dec}')$:

- $\text{Gen}'(1^n)$: Sample the key as follows: $k_1 \leftarrow \text{Gen}(1^n)$, $k_2 \leftarrow \{0, 1\}^n$ uniformly at random. Return (k_1, k_2) .
- $\text{Enc}'((k_1, k_2), m)$: Compute $c \leftarrow \text{Enc}(k_1, m)$. Return $(c, c \oplus k_2)$.
- $\text{Dec}'((k_1, k_2), (c_0, c_1))$: If $c_0 \oplus c_1 = k_2$, return $\text{Dec}(k_1, c_0)$, otherwise fail.

Determine whether Π' is CCA-secure, and prove your answer.

Question 5 (continued)

Name:

Solution: The scheme Π' is CCA-secure. Suppose, toward a contradiction, that a PPT adversary $\mathcal{A}$ wins the CCA game for Π' with non-negligible advantage. We construct a PPT adversary $\mathcal{B}$ that wins the CCA game for Π with the same advantage.

Adversary $\mathcal{B}$ samples $k_2 \xleftarrow{\$} \{0,1\}^n$ and runs $\mathcal{A}$. It simulates the oracles for $\mathcal{A}$ as follows:

- When $\mathcal{A}$ makes an encryption query m , adversary $\mathcal{B}$ forwards m to its own encryption oracle. If the response is c , it returns $(c, c \oplus k_2)$ to $\mathcal{A}$.
- When $\mathcal{A}$ makes a decryption query (c_0, c_1) , adversary $\mathcal{B}$ returns failure if $c_0 \oplus c_1 \neq k_2$. Otherwise, it queries its own decryption oracle on c_0 and returns the response to $\mathcal{A}$.

When $\mathcal{A}$ outputs challenge messages (m_0, m_1) , adversary $\mathcal{B}$ forwards them to its challenger. On receiving the base-scheme challenge ciphertext c^* , it gives

$$(c^*, c^* \oplus k_2)$$

to $\mathcal{A}$. Finally, $\mathcal{B}$ outputs the same guess b' as $\mathcal{A}$.

This simulation is perfect: the sampled value k_2 has the correct distribution, and every simulated encryption and decryption response is distributed exactly as in the real CCA game for Π' . It also respects the base game's restriction on decrypting c^* . Indeed, after receiving the challenge, the only valid Π' ciphertext whose first component is c^* is $(c^*, c^* \oplus k_2)$, which is exactly the challenge ciphertext and hence cannot be queried by $\mathcal{A}$. Any other pair beginning with c^* fails the validity check and is answered without querying $\mathcal{B}$'s decryption oracle.

Therefore

$$\Pr[\text{PrivK}_{\mathcal{B}, \Pi}^{\text{CCA}}(n) = 1] = \Pr[\text{PrivK}_{\mathcal{A}, \Pi'}^{\text{CCA}}(n) = 1].$$

Thus any non-negligible advantage against Π' would give the same non-negligible advantage against the CCA-secure scheme Π , a contradiction. Hence Π' is CCA-secure.