# Midterm I Solutions

**Name:**

**SID:**

- **Time: You have *1 hour and 20 minutes* (80 minutes) to complete the exam. The exam runs from 11:10 AM to 12:30 PM. No extra time will be given after 12:30 PM.**
- **After the exam starts, write your name and SID on every odd-numbered page. We reserve the right to deduct points if you do not, and you will not be allowed to do so after time is called.**
- **For short questions, your answers must be written clearly inside the box region. Any answer outside the box will not be graded. For longer questions, if you run out of space, you must clearly mention in the space provided for the question if part of your answer is elsewhere.**
- **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, and other electronic devices are NOT permitted for looking up content.**
- **There are 6 pages on the exam (counting this one). Notify a proctor immediately if a page is missing.**
- **We will not be answering questions during the exam. If you feel that something is unclear please write a note in your answer.**

1. Suppose $f, g : \{0,1\}^{2n} \to \{0,1\}^{2n}$ are one-way functions. For $x \in \{0,1\}^{2n}$, let $x = (x_1, x_2)$ be the left and right halves of $x$ of length $n$ with "," denoting concatenation, and let $\oplus$ be the bit-wise XOR operator.
   Answer and justify the following with proofs:

   (a) Let $\alpha(x) := (f(x), g(x))$. Is this a one-way function?

   No, not necessarily.

   **Counterexample:** Let $h : \{0,1\}^n \to \{0,1\}^n$ be any OWF and $x = (u, v) \in \{0,1\}^n \times \{0,1\}^n$. Define $f(u, v) := (h(u), v)$ and $g(u, v) := (u, h(v))$.

   $f, g$ are OWFs: Inverting either requires inverting $h$; given challenge $y$ for $h$, query the $f$-inverter on $(y, v)$ and extract the first component.

   $\alpha$ is not one-way: $\alpha(u, v) = \big((h(u), v), (u, h(v))\big)$ reveals $u$ and $v$ directly, so $\alpha$ is trivially invertible with probability 1.

   (b) Let $\beta(x) := f(x) \oplus x$. Is this a one-way function?

   Not necessarily.

   **Counterexample:** Let $h : \{0,1\}^n \to \{0,1\}^n$ be any OWF. Define $f(u, v) := (h(u),\ u \oplus v)$ for $(u, v) \in \{0,1\}^n \times \{0,1\}^n$.

   $f$ is a OWF: Inverting $f$ requires inverting $h$ on its first component. Reduction: given challenge $y$ for $h$, sample $v$, query the $f$-inverter on $(y, v)$; the first component of any preimage inverts $h$.

   $\beta$ is not one-way: $\beta(u, v) = f(u, v) \oplus (u, v) = (h(u) \oplus u,\ u)$.

   Given $y = (y_1, y_2) = \beta(u, v)$, the value $u = y_2$ is revealed directly. An adversary outputs $(y_2, 0^n)$; then $\beta(y_2, 0^n) = (h(y_2) \oplus y_2, y_2) = y$. This succeeds with probability 1, so $\beta$ is not one-way.

2. **Weak PRF definition.** In this question we will define weak PRF security and later construct a new weak PRF from a new number-theoretic assumption defined below. Let $F = \{F_n\}_{n\in\mathbb{N}}$ be an efficiently computable function ensemble with $F_n : \mathcal{K}_n \times \mathcal{X}_n \to \mathcal{Y}_n$. The weak PRF security game $\mathsf{wPRF}_F^{\mathcal{A}}(n)$ (for some $q$):

**Challenger:**

(a) Sample $b \xleftarrow{\$} \{0,1\}$, $k \xleftarrow{\$} \mathcal{K}_n$.

(b) Sample $x_1, \ldots, x_q \xleftarrow{\$} \mathcal{X}_n$ and $x^* \xleftarrow{\$} \mathcal{X}_n$ (challenge point).

(c) Let $y_i \leftarrow F_n(k, x_i)$ for $i = 1, \ldots, q$.

(d) If $b = 0$ set $y^* \leftarrow F_n(k, x^*)$; else $y^* \xleftarrow{\$} \mathcal{Y}_n$.

**Adversary $\mathcal{A}$:** receives $(1^n, (x_1, y_1), \ldots, (x_q, y_q), (x^*, y^*))$; outputs $b' \in \{0,1\}$.
**Outcome:** the game outputs 1 if $b' = b$, and 0 otherwise.

**Definition** (Weak PRF)**.** *$\{F_n\}_n$ is a* weak PRF (wPRF) *if for every PPT $\mathcal{A}$,*

$$\left|\Pr\left[\mathsf{wPRF}_F^{\mathcal{A}}(n) = 1\right] - \frac{1}{2}\right| \leq \mathsf{negl}(n).$$

**$q$-DDHI assumption.** Let $\{\mathbb{G}_n\}_{n\in\mathbb{N}}$ be an ensemble of groups. For $\mathbb{G}_n$, we let its generator be denoted by $g$ and its order be denoted by $p$. The $q$-DDHI game $q\text{-}\mathsf{DDHI}_{\mathbb{G}_n}^{\mathcal{D}}(n)$:

**Challenger:**

(a) Sample $b \xleftarrow{\$} \{0,1\}$, $\tau \xleftarrow{\$} \mathbb{Z}_p^*$.

(b) Compute $V \leftarrow (g, g^{\tau}, g^{\tau^2}, \ldots, g^{\tau^q})$.

(c) If $b = 0$ set $T \leftarrow g^{1/\tau}$; else $T \xleftarrow{\$} \mathbb{G}_n$.

**Adversary $\mathcal{D}$:** receives $(V, T)$; outputs $b' \in \{0,1\}$.
**Outcome:** the game outputs 1 if $b' = b$, and 0 otherwise.

**Definition** ($q$-DDHI)**.** *The* $q$-Decisional Diffie-Hellman Inversion ($q$-DDHI) assumption *holds for $\{\mathbb{G}_n\}_n$ if for every PPT $\mathcal{D}$,*

$$\left|\Pr\left[q\text{-}\mathsf{DDHI}_{\mathbb{G}_n}^{\mathcal{D}}(n) = 1\right] - \frac{1}{2}\right| \leq \mathsf{negl}(n).$$

**Problem.** We define the function ensemble $\{F_n\}_n$ by

$$F_n \colon (\mathbb{G}_n \times \mathbb{Z}_p) \times \mathbb{Z}_p \to \mathbb{G}_n, \qquad F_n((h,k),x) = h^{1/(k+x)},$$

where $p = |\mathbb{G}_n|$. **Prove** that $\{F_n\}_n$ is a secure wPRF according to the definition above.

**Reduction.** Given an adversary $\mathcal{A}$ that breaks the weak PRF, we construct an adversary $\mathcal{D}$ that breaks the $q$-DDHI assumption.

Adversary $\mathcal{D}(1^n, V, T)$ receives $V = (g, V_1, \ldots, V_q)$ and $T$ from the $q$-DDHI challenger. The code of $\mathcal{D}$:

**(1) For** $i = 1, \ldots, q$**:** sample $x_i \leftarrow$ $\mathbb{Z}_p$.

**(2) Sample** $x^* \leftarrow$ $\mathbb{Z}_p$.

**(3) Computation (if any):** For each $i$, set $u_i := x_i - x^*$. Let $P(z) := \prod_{i=1}^{q}(z + u_i) = \sum_{t=0}^{q} a_t z^t$. The coefficients $a_t \in \mathbb{Z}_p$ can be computed efficiently. Using the $q$-DDHI instance $V = (g, g^{\tau}, \ldots, g^{\tau^q})$, compute $h := g^{P(\tau)} = \prod_{t=0}^{q}(g^{\tau^t})^{a_t}$. This is possible since $\deg(P) = q$ and we have powers of $g^{\tau}$ up to $q$.
The implicit wPRF key is $(h, k)$ with $k := \tau - x^*$. Note that $\mathcal{D}$ does not know $\tau$ or $k$ explicitly, but can still compute $h$ from $V$.

**(4) For** $i = 1, \ldots, q$**:** set $y_i$ Since $(z + u_i)$ is a factor of $P(z)$, the quotient $P_i(z) := P(z)/(z + u_i)$ is a polynomial of degree $q - 1$ with known coefficients $c_{i,t}$.
Compute $y_i := g^{P_i(\tau)} = \prod_{t=0}^{q-1}(g^{\tau^t})^{c_{i,t}}$. This requires only powers up to $\tau^{q-1}$, which are available in $V$.

**(5) Set** $y^* =$ We need $y^* = h^{1/\tau} = g^{P(\tau)/\tau}$. Write $P(\tau)/\tau = \sum_{t=1}^{q} a_t \tau^{t-1} + a_0/\tau$. The first sum uses known powers; the $a_0/\tau$ term is where $T$ is embedded. Set:
$y^* := \left(\prod_{t=1}^{q}(g^{\tau^{t-1}})^{a_t}\right) \cdot T^{a_0}$.

**(6) Run** $b' \leftarrow \mathcal{A}\big(1^n, (x_1, y_1), \ldots, (x_q, y_q), (x^*, y^*)\big)$.

**(7) What does** $\mathcal{D}$ **output?** $b'$

**Argument that the reduction works:**

First, note that $x_1, \ldots, x_q, x^*$ are sampled uniformly and independently from $\mathbb{Z}_p$. Conditioned on no collisions among them (which holds with overwhelming probability since $|\mathbb{Z}_p|$ is super-polynomial), the inputs are distributed identically to the wPRF game.

With the implicit key $(h, k)$ where $k := \tau - x^*$ and $h := g^{P(\tau)}$, we have $k + x_i = \tau + u_i$ for each $i$. Step (4) computes $y_i = g^{P_i(\tau)} = g^{P(\tau)/(\tau+u_i)} = h^{1/(\tau+u_i)} = h^{1/(k+x_i)} = F_n((h, k), x_i)$, which is exactly the correct wPRF evaluation.

**Case** $b = 0$**:** $T = g^{1/\tau}$, so step (5) yields $y^* = g^{P(\tau)/\tau} = h^{1/\tau} = h^{1/(k+x^*)} = F_n((h, k), x^*)$. This is consistent with the real wPRF game.

**Case** $b = 1$**:** $T$ is uniform in $\mathbb{G}_n$. Since $a_0 = \prod_{i=1}^{q} u_i \neq 0$ with overwhelming probability (each $u_i = x_i - x^* \neq 0$ conditioned on no collisions), $T^{a_0}$ is also uniform, making $y^*$ uniformly random and independent of the other values. This is consistent with the random wPRF game.

Therefore $\mathcal{A}$'s view under $\mathcal{D}$'s simulation is identical to the wPRF game (up to negligible collision probability), so $\mathbf{Adv}^{q\text{-DDHI}}(\mathcal{D}) = \mathbf{Adv}^{\text{wPRF}}(\mathcal{A}) - \mathsf{negl}(n)$. If $\mathcal{A}$ has non-negligible wPRF advantage, then $\mathcal{D}$ breaks $q$-DDHI, a contradiction. Hence $\{F_n\}_n$ is a secure wPRF.

3. **LOR-CPA security** Let $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ be a symmetric encryption scheme.

The game $\mathsf{LOR\text{-}CPA}^{\mathcal{A}}_{\Pi}(\lambda)$ proceeds as follows:

(a) $b \xleftarrow{\$} \{0,1\}$; $k \leftarrow \mathcal{G}(1^\lambda)$

(b) $\mathcal{A}$ has access to oracle $\mathcal{O}_{k,b}(\cdot,\cdot)$ which does the following:

- On input $(m_0, m_1)$ with $|m_0| = |m_1|$, returns $c \leftarrow \text{Enc}(k, m_b)$

(c) $\mathcal{A}$ makes $Q$ queries to $\mathcal{O}_{k,b}$ and outputs $b'$

(d) Output 1 iff $b' = b$ and 0 otherwise

Prove that $\Pi$ is LOR-CPA secure if and only if it is IND-CPA secure. Provide reductions and justifications for both directions.

**Direction 1: LOR-CPA $\Rightarrow$ IND-CPA.** (If $\Pi$ is LOR-CPA secure then $\Pi$ is IND-CPA secure.)

Assume $\Pi$ is LOR-CPA secure. Let $\mathcal{A}$ be a PPT adversary against IND-CPA. We construct a PPT adversary $\mathcal{B}$ against LOR-CPA such that $\mathcal{B}$ runs $\mathcal{A}$ and:

$\mathcal{B}$ simulates IND-CPA for $\mathcal{A}$ using the LOR oracle:

**Encryption queries:** On query $m$, return $\mathcal{O}_{k,b}(m,m) = \text{Enc}_k(m)$ (independent of $b$, perfect simulation).

**Challenge:** On $(m_0, m_1)$, query $\mathcal{O}_{k,b}(m_0, m_1)$ and return $c^* = \text{Enc}_k(m_b)$.

**Output:** $\mathcal{B}$ outputs $\mathcal{A}$'s guess $b'$.

This is a perfect IND-CPA simulation with the same hidden bit $b$, hence $\mathbf{Adv}^{\text{IND-CPA}}_{\Pi}(\mathcal{A}) = \mathbf{Adv}^{\text{LOR-CPA}}_{\Pi}(\mathcal{B})$, so LOR-CPA security implies IND-CPA security.

**Direction 2: IND-CPA $\Rightarrow$ LOR-CPA.** (If $\Pi$ is IND-CPA secure then $\Pi$ is LOR-CPA secure.)

Assume $\Pi$ is IND-CPA secure. Let $\mathcal{A}$ be a PPT adversary against LOR-CPA making $Q$ queries such that $\varepsilon := \mathbf{Adv}^{\text{LOR-CPA}}_{\Pi}(\mathcal{A})$ is non-negligible. We construct a PPT adversary $\mathcal{B}$ against IND-CPA such that $\mathcal{B}$ runs $\mathcal{A}$ and:

Define hybrids $H_j$ for $j = 0, \ldots, Q$: in $H_j$, the $i$-th LOR query $(m_0^{(i)}, m_1^{(i)})$ is answered with $\text{Enc}_k(m_1^{(i)})$ if $i \le j$ and with $\text{Enc}_k(m_0^{(i)})$ if $i > j$. Thus $H_0$ encrypts only left messages ($b = 0$) and $H_Q$ encrypts only right messages ($b = 1$).

Let $\Delta_j := |\Pr[\mathcal{A} \to 1 \text{ in } H_j] - \Pr[\mathcal{A} \to 1 \text{ in } H_{j-1}]|$. Telescoping and using the triangle inequality gives $\sum_j \Delta_j \ge \varepsilon$, so some $t$ satisfies $\Delta_t \ge \varepsilon/Q$ (which is non-negligible since $Q$ is polynomial). We now use this difference to build an IND-CPA adversary $\mathcal{B}_t$.

**Building $\mathcal{B}_t$:** Run $\mathcal{A}$; for $i < t$ answer with $\text{Enc}_k(m_1^{(i)})$; for $i > t$ answer with $\text{Enc}_k(m_0^{(i)})$; for $i = t$ submit $(m_0^{(t)}, m_1^{(t)})$ as IND-CPA challenge.

When the IND bit is 0, $\mathcal{B}_t$'s view is identical to $H_{t-1}$ while when the IND bit is 1 it is identical to $H_t$, hence $\mathbf{Adv}^{\text{IND-CPA}}_{\Pi}(\mathcal{B}_t) = \Delta_t \ge \varepsilon/Q$.

Hence, $\mathbf{Adv}^{\text{IND-CPA}}_{\Pi}(\mathcal{B}) \ge \varepsilon/Q$ is non-negligible, contradicting IND-CPA security. Therefore IND-CPA $\Rightarrow$ LOR-CPA.