UC Berkeley — CS 276 : Cryptography
Prof. Sanjam Garg

Midterm II

Midterm II
March 19, 2026

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. **[25 points]** Let $\mathcal{H} = \{h_s : \{0,1\}^{2n} \to \{0,1\}^n\}_{s \in \{0,1\}^k}$ be a UOWHF, where k is polynomial in n. Define the composed family

$$\mathcal{F} = \{f_{s_1,s_2,s_3} : \{0,1\}^{4n} \to \{0,1\}^n\}_{s_1,s_2,s_3 \in \{0,1\}^k}$$

defined by

$$f_{s_1,s_2,s_3}(x_L \| x_R) = h_{s_3}(h_{s_1}(x_L) \| h_{s_2}(x_R)),$$

where $x_L, x_R \in \{0,1\}^{2n}$.

Is $\mathcal{F}$ necessarily a UOWHF?

Either prove it or give a counterexample family.

2. **[25 points] Existential Unforgeability under Known Message Attack (EUF-KMA).** Let $\Pi = (\text{Gen}, \text{Sign}, \text{Verify})$ be a signature scheme. The EUF-KMA game $\mathsf{EUF\text{-}KMA}^{\mathcal{A}}_{\Pi}(n)$ proceeds as follows:

Game $\mathsf{EUF\text{-}KMA}^{\mathcal{A}}_{\Pi}(n)$

(a) Challenger samples $(vk, sk) \leftarrow \text{Gen}(1^n)$ and sends vk to $\mathcal{A}$.

(b) **Message Queries:** $\mathcal{A}$ sends messages $m^{(1)}, \ldots, m^{(q)}$ to the challenger. The challenger computes $\sigma^{(i)} \leftarrow \text{Sign}(sk, m^{(i)})$ for all $i \in \{1, \ldots, q\}$ and returns the signatures $(\sigma^{(1)}, \ldots, \sigma^{(q)})$ to $\mathcal{A}$.

(c) **Forgery:** $\mathcal{A}$ outputs (m^*, σ^*).

(d) $\mathcal{A}$ outputs 1 if $\text{Verify}(vk, m^*, \sigma^*) = 1 \wedge m^* \notin \{m^{(1)}, \ldots, m^{(q)}\}$ and 0 otherwise.

Definition (EUF-KMA). Π is *Existentially Unforgeable under Known Message Attack (EUF-KMA)* if for every PPT adversary $\mathcal{A}$

$$\Pr[\mathsf{EUF\text{-}KMA}^{\mathcal{A}}_{\Pi}(n) = 1]$$

is a negligible function in n.

Given a signature scheme $\Pi = (\text{Gen}, \text{Sign}, \text{Verify})$ that is EUF-KMA secure, and a hash function H (modeled as a random oracle), construct a signature scheme $\Pi' = (\text{Gen}', \text{Sign}', \text{Verify}')$ that is EUF-CMA secure in the Random Oracle model.

Construction of Π': Outline Gen', Sign', and Verify'.

$\text{Gen}'(1^n)$: Run $(vk, sk) \leftarrow \text{Gen}(1^n)$. Output [ ]

$\text{Sign}'(sk, m)$: Compute [ ] and output [ ]

$\text{Verify}'(vk, m, \sigma)$: Compute [ ] and output [ ]

Proof of Security:

Proof of Security (continued):

3. **[50 points] Combining Public Key Encryption Schemes.**
Let $\Pi_A = (\text{Gen}_A, \text{Enc}_A, \text{Dec}_A)$ and $\Pi_B = (\text{Gen}_B, \text{Enc}_B, \text{Dec}_B)$ be two public-key encryption (PKE) schemes. Assume that *at least one* of these schemes is IND-CPA secure (but not knowing which one).

   (a) **[15 points]** Construct an IND-CPA secure PKE scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$.

   Gen(1^n)**:**

   Run $(pk_A, sk_A) \leftarrow \text{Gen}_A(1^n)$ and $(pk_B, sk_B) \leftarrow \text{Gen}_B(1^n)$.

   Output

   Enc(pk, m)**:**

   Compute

   Run $c_A \leftarrow \text{Enc}_A(pk_A,$) and $c_B \leftarrow \text{Enc}_B(pk_B,$).

   Output

   Dec(sk, c)**:**

   Parse c as .

   Compute $\leftarrow \text{Dec}_A(sk_A, c_A)$ and $\leftarrow \text{Dec}_B(sk_B, c_B)$.

   Output

(b) **[20 points]** Prove that your construction from part (a) is IND-CPA secure.

(c) **[15 points]** Assuming both Π_A and Π_B are *IND-CCA2* secure, is your construction from part (a) IND-CCA2 secure? Justify your answer, and if not, demonstrate an attack.