CS 601.442/642 – Modern Cryptography Instructors: Aditya Hegde and Harry Eldridge

Extra Credit Homework

Deadline: April 24; 2026 11:59pm ET

Instructions

- This is an *extra credit* homework. Answer as many questions as you would like. All correct answers will be counted as extra credit.

Problems

1. (10 points) In this problem we will see why a natural idea for constructing an IND-CCA-2 secure public key encryption scheme does not work. Let $(\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ be an IND-CPA secure public key encryption scheme, and let $(\mathsf{DSKeyGen}, \mathsf{Sign}, \mathsf{Ver})$ be a strong UF-CMA secure digital signature scheme. We define a new public key encryption scheme $(\mathsf{KGen}', \mathsf{Enc}', \mathsf{Dec}')$ below.

$\mathsf{KGen}'(1^\lambda)$	$\mathsf{Enc}'(\mathsf{pk}, m)$	$\mathsf{Dec}'(\mathsf{sk}, (\mathsf{pk}_{sig}, \mathsf{ct}, \sigma))$
1 : return $\mathsf{KGen}(1^\lambda)$	1 : $(\mathsf{sk}_{sig}, \mathsf{pk}_{sig}) \leftarrow \mathsf{DSKeyGen}(1^\lambda)$	1 : if $\mathsf{Ver}(\mathsf{pk}_{sig}, \mathsf{ct}, \sigma) \neq 1$ then return $\perp$
	2 : $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$	2 : else return $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$
	3 : $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}_{sig}, \mathsf{ct})$	
	4 : return $(\mathsf{pk}_{sig}, \mathsf{ct}, \sigma)$	

   Prove that $(\mathsf{KGen}', \mathsf{Enc}', \mathsf{Dec}')$ does *not* satisfy IND-CCA-2 security.

2. (10 points) We say that a public key encryption scheme $(\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ is *additively homomorphic* if for all $m_0, m_1 \in \mathcal{M}$:

$$\Pr\left[\mathsf{Dec}(sk, \mathsf{ct}_0 + \mathsf{ct}_1) = m_0 + m_1 \ : \ \begin{array}{r}(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}(1^\lambda) \\ \mathsf{ct}_0 \leftarrow \mathsf{Enc}(\mathsf{pk}, m_0) \\ \mathsf{ct}_1 \leftarrow \mathsf{Enc}(\mathsf{pk}, m_1)\end{array}\right] = 1$$

   Let $\Pi = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ be an additively homomorphic IND-CPA secure encryption scheme with message space $\mathcal{M} = \mathbb{Z}_p$. Prove that Π does *not* satisfies IND-CCA-2 security.

3. (10 points) Let $(\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme. We can construct a new encryption scheme $(\mathsf{KGen}', \mathsf{Enc}', \mathsf{Dec}')$ for ℓ-bit messages as follows:

$\mathsf{KGen}'(1^\lambda)$	$\mathsf{Enc}'(k, m; r)$	$\mathsf{Dec}'(k, \mathsf{ct})$
1 : return $\mathsf{KGen}(1^\lambda)$	1 : return $\mathsf{Enc}(k, m\|\|r; r)$	1 : return $\mathsf{Dec}(k, \mathsf{ct})[:\ell]$

   Recall that the notation $\mathsf{Enc}(k, m; r)$ means explicitly defining the randomness used in Enc. You may assume that $r \in \{0,1\}^\lambda$, and therefore that executing $\mathsf{Enc}(k, m)$ is equivalent to first sampling $r \leftarrow\!\!\$\ \{0,1\}^\lambda$ and then running $\mathsf{Enc}(k, m; r)$.

   We will prove that the above construction is not secure.

(a) Let $(\mathsf{KGen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ be an IND-CPA secure encryption scheme. Construct an encryption scheme $(\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$, and briefly justify why it is correct and satisfies IND-CPA security (you do no need to write a formal proof).

(b) Prove that when $(\mathsf{KGen}', \mathsf{Enc}', \mathsf{Dec}')$ is instantiated with your scheme the resulting scheme does *not* satisfy IND-CPA security.

4. (20 points) Suppose a family of functions $H = \{h_i : \{0,1\}^{2\lambda} \to \{0,1\}^{\lambda}\}$ has the following property: for all h_i, it is the case for all $x, y \in \{0,1\}^{2\lambda}$ that if $x \leq y$ then $h_i(x) \leq h_i(y)$. Prove that H is *not* a collision resistant hash function family. Your proof should give an explicit collision-finding attack against H.

5. (20 points) Suppose that Alice and Bob hold correlated inputs of the following form: Alice has (r_0, r_1), where each $r_i \leftarrow\!\!\$\ \{0,1\}$ and Bob has (c, r_c), where $c \leftarrow\!\!\$\ \{0,1\}$.

   Further suppose that at a later point, Alice and Bob wish to securely compute 1-out-of-2 OT with inputs (x_0, x_1) and b respectively (assume that x_0 and x_1 are also single bits). Show how Alice and Bob can use their correlated inputs to perform this task without using any cryptographic assumptions. That is, design a protocol for 1-out-of-2 OT that achieves *unconditional* security against semi-honest adversaries. Argue correctness and security of your protocol. (You don't need to give a full formal proof.)

   Hint: Recall that one-time pads do not require any cryptographic assumptions.

6. (10 points) Let Alice and Bob be two parties with inputs $z \in \mathbb{Z}_p$ and $b \in Z_p$, respectively. They wish to check whether their inputs are equal, i.e. whether $a = b$. They want to do this while making sure they do not learn any other information about the other party's input. In other words, if $a \neq b$, then Alice should not learn anything about b and Bob should not learn anything about a.

   Let $\mathbb{G}$ be a cyclic croup of prime order p with generator g. Alice and Bob run the following protocol:

   - Alice samples a random value $r \leftarrow\!\!\$\ \mathbb{Z}_q$. She then computes $X = g^r$ and $Y = g^{ar}$. She sends (X, Y) to Bobe.
   - Bob computes X^b. He outputs 1 if $X^b = Y$, and 0 otherwise.

   Explain why this protocol is not secure against a semi-honest Bob.

7. (20 points) Let Alice and Bob have inputs a and b, respectively. They want to securely send $(a + b)$ to a third-party Carol. Devise a protocol where Alice and Bob are only allowed to send **at most one message to each other** and **at most one message each to Carol**. Your protocol should satisfy all of the following security properties:

   - *Security against semi-honest Alice*: Alice should not learn b.
   - *Security against semi-honest Bob*: Bob should not learn a.
   - *Security against semi-honest Carol*: Carol should not learn a or b.

   Argue that your protocol indeed satisfies all three security conditions, and gives the correct output to Carol. (You do not need to give a formal proof.)