隐私计算与数据合规（2024-2025）期末

A 卷

一、单选题（下列选项中仅有一个选项是正确的）

1. If $a \equiv b \pmod{n}$, and $c \in \mathbb{Z}$, then

   (A) $ac \equiv bc \pmod{n}$

   (B) $a = b$

   (C) $ac \neq bc \pmod{n}$

   (D) $a \neq b$

2. El-Gamal encryption is IND-CPA (indistinguishable chosen plaintext attack) secure under which assumption

   (A) Discrete logarithm

   (B) Factoring

   (C) Computational Diffie-Hellman

   (D) Decisional Diffie-Hellman

3. Which of the following techniques is NOT a trusted hardware?

   (A) Zero-knowledge proof

   (B) Trusted Platform Modules (TPM)

   (C) ARM TrustZone

   (D) Intel SGX

4. Which of the following protocols is to privately compute the intersection of two sets:

   (A) PSI

   (B) PIR

   (C) Encrypted database

   (D) Federated learning

二、不定项选择题（下列选项中至少有一个选项是正确的，少选或多选均不得分）

1. Choose all correct descriptions for Zero-knowledge proofs from the followings.

   (A) Zero-knowledge proofs have interactive and non-interactive two types.

   (B) All zero-knowledge proofs must repeat multiple times to have high enough soundness.

   (C) Zero-knowledge proofs do not leak any information to the verifier.

   (D) The security of zero-knowledge proofs can be guaranteed against computationally unbounded adversaries.

2. Lifted El-Gamal encryption is a modification of El-Gamal encryption; namely, encrypting of ”instead of m. Choose all correct descriptions.

   (A) Lifted El-Gamal encryption is additively homomorphic.

   (B) The security assumption of lifted El-Gamal encryption is the same as El-Gamal encryption.

   (C) Lifted El-Gamal cannot be used to encryption large plaintext; otherwise, the description may fail.

   (D) The security of lifted El-Gamal can be reduced to the discrete logarithm assumption.

3. Choose the building blocks for secure two/multi party computation:

   (A) OT

   (B) Garbled Circuit

   (C) Secret Sharing

   (D) Private set intersection

4. Choose all correct descriptions for universal composability security framework from the followings:

   (A) Protocols with universal composability is information theoretical secure.

   (B) Protocols with universal composability can be executed concurrently.

   (C) Universal composability is a framework for proving protocol security.

   (D) Universal composability is a simulation-based security definition.

三、问答题

1. Alice holds input $A = (a_1, a_2, \ldots, a_n)$, Bob holds input $B = (b_1, b_2, \ldots, b_n)$. Design a two-party protocol that allows Alice and Bob to jointly compute the inner product of A and B (i.e., $\sum_{i=1}^{n} a_i * b_i$) without leaking their input to each other.

2. What is the security definition of the oblivious transfer protocol? Given a secure (1,2)-OT, (i.e. 1-out-of-2 oblivious transfer protocol,) could you construct a (1,4)-OT protocol? And show why the proposed a (1,4)-OT protocol is secure.

3. Explain why the following protocol is insecure:
   Alice has a set $(x_1, x_2, \ldots, x_i)$ and Bob has a set $(y_1, y_2, \ldots, y_i)$. To compute intersection, Alice sends $(H(x_1), H(x_2), \ldots, H(x_i))$ to Bob, where $H()$ is a cryptographic hash function. Bob computes the intersection between $(H(y_1), H(y_2), \ldots, H(y_i))$ and $(H(x_1), H(x_2), \ldots, H(x_i))$.

4. Describe the SPDZ protocol for $P_1, \ldots, P_n$ to jointly evaluate the function $y = f(x_1, \ldots, x_n)$, where x_i is the private input of P_i.

分数：

- 单选题：$4 + 4 = 16$
- 多选题：$6 + 4 = 24$
- 问答题：$15 + 4 = 60$