Week 5 Assignment 5
The due date for submitting this assignment has passed.

Due on 2021-09-01, 23:59 IST.

As per our records you have not submitted this assignment.

1. Understand the following fact: any of the point-processed model for spatial-standard evaluation?

2. The question is multiple-choice, where a = 0, x 

3. Consider the following two statements about the degree reduction problem:

   (a) The degree-reduction problem can be solved non-interactively.
   (b) The degree-reduction problem consists of computing a scalar a, 1 if Shannor sharing of a is involved.

Which of his followings option is correct?

   - Both (a) and (b) are correct
   - Both (a) and (b) are incorrect
   - (a) is correct but (b) is incorrect
   - (b) is correct but (a) is incorrect

No. the answer is incorrect.

4. Accepted Answer

   (a) is correct but (b) is incorrect

5. Let \( \mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3 \) be \( \mathcal{P} = \{ 1, 2, \ldots, n \} \) parties out of which an adversary corrupts \( c \) parties. In order to generate correlated randomness [Referees, Triplets, the parties perform the following protocol denoted as 'Shannor':

   - Protocol 'Shannor' generates an \((a, b, c)\)-Shannor sharing of a multiplication triple \((a, b, c)\), such that \( c = a \cdot b \) but \( a \) and \( b \) are not uniformly random field elements.

   Protocol 'Shannor' requires communication of \(O(n^2)\) field elements.

   Protocol 'Shannor' can be performed with \(O(n)\) rounds of communication.

   No. the answer is incorrect.

   Accepted Answer

   Protocol 'Shannor' requires communication of \(O(n^2)\) field elements.

   Protocol 'Shannor' can be performed with \(O(n)\) rounds of communication.

6. Let \( \mathcal{H}_1, \mathcal{H}_2 \) denote the set of all possible messages exchanged between two parties in protocol for computing OR of input bits \( b_1 \) and \( b_2 \) with perfect security. Consider the following statements:

   \[ (a) \; \mathcal{H}_1 \cap \mathcal{H}_2 = \emptyset \]

   \[ (b) \; \mathcal{H}_1 \cap \mathcal{H}_2 = \{0,1 \} \]

   Choose the most appropriate option:

   - Only (a) true
   - Only (b) true
   - Both (a) and (b) are true
   - Both (a) and (b) are false

   No. the answer is incorrect.

   Accepted Answer

   Both (a) and (b) are true.

7. Let \( \mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3 \) be \( \mathcal{P} = \{ 1, 2, \ldots, n \} \) parties out of which an adversary corrupts \( c \) parties. These parties hold an \((a, b, c)\)-sharing of two inputs \( a \) and \( b \) denoted as \( \mathcal{S}(a, b, c) \) and \( \mathcal{S}(a', b', c') \) respectively and wish to compute a random \( (a, b) \)-sharing of the product \( c = a \cdot b \) denoted as \( \mathcal{S}(a, b) \) such that each new additional information about \( a \) and \( b \) is leaked to the adversary.

   Assume additionally that the parties hold the \((a, b)\)-sharing of an \(\mathcal{S}(a, b)\) unknown uniformly random field element \( r \) defined as \( r \) and hold \((a, b, c)\)-shares of the same element \( r \) denoted as \( r' \). The parties perform the following protocol denoted as 'Mulsh':

   (1) The parties locally compute \( (a, b, c)\)-shares of the value \( v = a \cdot b \) denoted as \( (a', b', c') \) by multiplying their shares of \( a \) and \( b \) that is \( (a', b', c') = (a \cdot b, b', c') \).

   (2) The parties send their \((a, b)\)-shares of \( v \) to the party \( \mathcal{P}_1 \).

   (3) \( \mathcal{P}_1 \) reconstructs the secret \( v \) using the shares it receives from \( \{ \mathcal{P}_1 \} \) and its own share and sends \( (a, b) \)-shares to all parties.

   (4) All the parties now locally compute \((a, b)\)-shares of \( v = a \cdot b \) computing:

   \[ a' = a \cdot b \]

   Note that all the sharings used above are Shamir sharings.

   Which of the following options is correct regarding Mulsh?

   - If \( \mathcal{P}_1 \) is a corrupt party, then the protocol Mulsh leaks the value of \( a \) and \( b \) to the adversary.

   The protocol Mulsh solves the degree reduction problem, that is, after running Mulsh, the parties are able to obtain a random \((a, b)\) Shamir sharing of \( c = a \cdot b \) given a \((a, c)\) Shamir sharing of \( a \) and \( b \) without leaking any information about \( a \) or \( b \) if the value \( r \) is known to the adversary then the protocol Mulsh does not leak any additional information about \( a \) and \( b \) respectively.

   No. the answer is incorrect.

   Accepted Answer

   Protocol 'Shannor' solves the degree reduction problem, that is, after running Mulsh, the parties are able to obtain a random \((a, b)\) Shamir sharing of \( c = a \cdot b \) given a \((a, c)\) Shamir sharing of \( a \) and \( b \) without leaking any information about \( a \) or \( b \) if the value \( r \) is known to the adversary then the protocol Mulsh does not leak any additional information about \( a \) and \( b \).