Lecture #5 Exercises

Distributed Lab

August 20, 2024

Exercise 1. Dmytro and Denis were watching a horse race. Confident in his ability to predict the outcome, Dmytro decided to commit to his prediction. However, in his haste, he forgot to use a blinding factor. Now, Dmytro is concerned that Denis might discover his prediction before the race ends, which would defeat the purpose of his commitment.

We define a dummy hash function $H(a) = (a \cdot 13 + 17) \pmod{41}$. Dmytro used a *hash-based commitment* and H as a hash function. Set of race horse numbers is $(3, 5, 8, 15)$. Help Denis to find out the horse number Dmytro have made a commitment to, if commitment equals $C = 39$.

(A) 3.

(B) 5.

(C) 8.

(D) 15.

Exercise 2. Denis made a setup (points G and U) for a Pedersen commitment scheme and commited values $(3, 7)$ to Dmytro by sending him $\mathcal{C} = [3]G + [7]U$. Dmytro did not verify the setup. turns out that Denis knows that $U = [6]G$. He wants to change the committed message to 15. Which values (m, r) should he send to Dmytro at the opening stage?

(A) $(15, 5)$

(B) $(15, 7)$

(C) $(15, 4)$

(D) $(3, 5)$

Exercise 3. We define a dummy hash function $H(a, b) = (a \cdot 3 + b \cdot 7) \pmod{41}$. You have a Merkle tree built with depth 4 using hash function H with root equal 37. Which inclusion proof is valid for element 3? Position defines how leaves should be hashed:

- if $left \to h_i = Hash(h_{i-1}, branch[i])$

- if $right \to h_i = Hash(branch[i], h_{i-1})$

(A) branch: $[4, 16, 13]$, position: $[left, right, left]$

(B) branch: $[1, 40, 3]$, position: $[left, left, left]$

(C) branch: $[5, 12, 13]$, position: $[right, right, left]$

(D) branch: $[4, 17, 13]$, position: $[left, right, left]$

Exercise 4. Given a polynomial $p(x) = x^3 - 10x^2 + 31x - 30$, Oleksandr wants to prove that $p(2) = 0$. To do that, according to the KZG commitment scheme, he constructs the quotient polynomial $q(x)$ and wants to show that $q(\tau) \cdot (\tau - 2) = p(\tau)$. Assuming Oleksandr has conducted these steps correctly, what value of $q(x)$ has Oleksandr calculated?

(A) $q(x) = 2x^2 + 4x - 6$

(B) $q(x) = x^3 - 10x^2 + 30x - 28$

(C) $q(x) = x^2 - 8x + 15$

(D) $q(x) = x^2 + 5x + 18$