Lecture #5 Exercises

Distributed Lab

August 20, 2024

Exercise 1. Denis decided to commit to the race results, but forgot to use the blinding factor. He used a hash-based commitment and SHA256 hash function. Set of race participant numbers: $(0x1, 0x3, 0x8, 0x15)$. Can you break the hiding property of the commitment? Select the participant number Denis made a commitment to, if

$\mathcal{C} = 0xbeead77994cf573341ec17b58bbf7eb34d2711c993c1d976b128b3188dc1829a$.

(A) $0x1$.

(B) $0x3$.

(C) $0x8$.

(D) $0x15$.

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. It turns out that Denis knows the discrete logarithm of $U = [6]G$. 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) $(3, 7)$

(E) $(3, 5)$

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

(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 $p(x) = x^3 - 10x^2 + 31x - 30$, you want to prove that $p(2) = 0$. Calculate a *quotient* polynomial.

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

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

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

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