ZK Bootcamp: Day 3 Problem Set

Brian Justin Stout[*]

July 31, 2023

Problem 1. *Use the example file to generate a proof to show that the prover knows the squareroot of 25.*

A Groth16 proof consists of three points on an elliptic curve:

$$\begin{gathered}
[\text{“}0x168ac11550698217d0a8c8dccb9d63222a0eeb078af62d80f65455a043458761\text{”}, \\
\text{“}0x2f63877dbc29a005f64b36150aa45df93fe6efbbd0489515422f0ebcd75ab6e0\text{”}], \\
[\text{“}0x0b77da1e3bad32fd19506192be3c6e06854f3a3ea7c758dc27805858e3220566\text{”}, \\
\text{“}0x2dcf7b563604a15c0cbaa1404484386a8e17a4b06cab808ac8f588053c9ee444\text{”}], \\
[\text{“}0x065a50275b2cb4b83333accc62b9f0ed8da9a15cf0d888d516ca9fd14cc0dc60\text{”}, \\
\text{“}0x2f9c1ef1447c957611090cf6fed96ae0333332c747d333f0d145ca429f2d4221\text{”}], \\
[\text{“}0x288319fa71c2f6d7a6c97fdfd146752fcf2e8344add536e1ea403b294fc2ec8d\text{”}, \\
\text{“}0x162591b99034169b13646616ef2cc177b0cc56c3b00cb9641de0003ab81ac1fb\text{”}]
\end{gathered}$$

Problem 2. *Try to create an invalid proof.*

If we try to create an invalid proof, say with an a such that $a^2! = b$, then the compute stage fails and we cannot continue with the set up and proof generation.

Problem 3. *Follow the example to build a proof that you know the pre-image of a hash.*

We can use the sha256packed function in the Zokrates stdlib to compute a hash. We then need to assert that the computed hash on the private inputs match the specified hash. We get the following proof of the knowledge preimage of the hash of

$$0xc6481e22c5ff4164af680b8cfaa5e8ed3120eeff89c4f307c4a6faaae059ce10$$

.

[*] email: bstout.eth@ethermail.io

$$\begin{gathered}
“a” : [“0x1dd7d1baa67b3ad618af2c3b0eb353ce0721283207b7d57f373dd76b610ee3db”,\\
“0x05d7e06c0d9e58b7a8df87632fb01aaa92e9e66091cd3ee4c149a1baa41628c5”],\\
“b” : [[“0x165fb8e6711f99474f30dd5312592d58b693da908b32ad9cfdff1af090a1c461”,\\
“0x0d66710dd6a4f9669808c6e0a7b1ceec2c3113b1786c9db52100c929c6e06f51”],\\
[“0x197ac699571e0d0446b4cf01b28a1cc20c2125a194ea952e56c6a16b8b4ee230”,\\
“0x2108f9bc5897143461813bfed0f70278a4c53db4aaf709c02566ed1177463889”]],\\
“c” : [“0x203eb50d9e04ff587982e5efbc54d7e04f076f43b856806b08340e7a23200781”,,\\
“0x030d4b1d779ed834f22a84c44dedc2b6039d7b87a809e84a169e96bd89dcc797”]
\end{gathered}$$

Problem 4. *In principle how could you use Zokrates to verify that a certain address on Ethereum has more than say 1 ETH.*

If E is an ethereum address, then we could read $E.balance$ from the ethereum network. We would then use Zokrates to assert that $E.balance > 1000000000000000000$.