Zero Knowledge Bootcamp

#5. Homomorphic encryption and EC arithmetic in Solidity

RareSkills

Homomorphic encryption

Alice wants to prove to Bob that she knows two numbers whose sum is 12. Instead of sending the two numbers, say a and b, she sends the corresponding points on the elliptic curve.

$$\text{points } aG, bG$$

$$aG + bG = (a + b)G$$

RareSkills

A set of equations

It is possible to do the same with a system of equations

$$
\begin{aligned}
x + y + z &= 6 \\
2x + 3y + z &= 11 \\
x + 2y + 3z &= 14
\end{aligned}
$$

$$
\begin{bmatrix} 1 & 1 & 1 \\ 2 & 3 & 1 \\ 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 6 \\ 11 \\ 14 \end{bmatrix}
$$

RareSkills

Alice will send G, 2G and 3G to Bob, and Bob will verify if

$$G + 2G + 3G = 6G$$
$$2 \cdot G + 3 \cdot 2G + 3G = 11G$$
$$G + 2 \cdot 2G + 3 \cdot 3G = 14G$$

$$x + y + z = 6$$
$$2x + 3y + z = 11$$
$$x + 2y + 3z = 14$$

“Problems” with this approach

- Alice needs to send all the numbers to Bob, it's not succinct
- The equations are linear, meaning we can't deal with multiplication (yet)

RareSkills

A problem with multiplication...

Alice wants to prove to Bob that she knows three numbers whose multiplication is 12.

$$3 \cdot 2 \cdot 2 = 12$$

$$3G, 2G, 2G \rightarrow \text{Bob}$$

$$\text{Bob can't } 3G \cdot 2G \cdot 2G$$

RareSkills

EC arithmetic in Solidity

eccAdd (address 6)

To calculate P + Q you need to send the coordinates (x,y), each value as uint256, of P and Q, in order, ABI encoded. The result will be (uint256, uint256).

RareSkills

EC arithmetic in Solidity

eccMul (address 7)

To calculate nP you need to send the coordinates (x,y), each value as uint256, of P, n as uint256, in order, ABI encoded. The result will be (uint256, uint256).

RareSkills