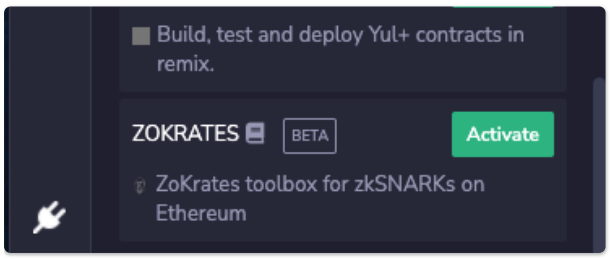
Homework 3

Practice using Zokrates

Use [Remix]

Install the Zokrates plugin



1. Use the example file to generate a proof to show that a prover knows the square root of 25.
2. Try to create an invalid proof
3. Follow the example to build a proof that you know the pre image of a hash https://zokrates.github.io/examples/sha256example.html
4. In principle how could you use Zokrates to verify that a certain address on Ethereum has more than say 1 ETH ?

4)

Create a ZoKrates program in a .zok file. In this program, we'll check if an Ethereum address has a balance greater than 1 ETH (1 ETH = 1e18 wei).

```
def main(public field balance):
    isMoreThanOneETH = if balance > 1000000000000000000 then 1 else 0 fi
return isMoreThanOneETH
```

Use ZoKrates to compile the ZoKrates program and generate the proving key, verification key, and a zero-knowledge proof for a specific address.

Write an Ethereum smart contract that includes a function for verifying the proof and a function for checking the balance of an Ethereum address.

Deploy the smart contract to the Ethereum network and set the verifying key. You can then use the `checkBalance` function to verify whether a specific address has more than 1 ETH.