

Project on Cryptography

Section1--Document

Team: Code clash

Objective:

To demonstrate creating and verifying a Zero Knowledge Proof (ZKP) to prove knowledge of a SHA256 hash pre-image without revealing the secret, highlighting ZKPs' use in secure authentication.

Execution of commands in terminal

Installing zokrates

```
pms@LAPTOP-RNATB7H7:~$ curl -LSfs get.zokrat.es | sh
ZoKrates: Tag: latest (0.8.8)
ZoKrates: Detected architecture: x86_64-unknown-linux-gnu
ZoKrates: Installing to: /home/pms/.zokrates
ZoKrates: Fetching: https://github.com/ZoKrates/ZoKrates/releases/download/0.8.8/zokrates-0.8.8-x86_64-unknown-linux-gnu.tar.gz
ZoKrates is already installed, overwrite (y/n)? y

ZoKrates was installed successfully!
If this is the first time you're installing ZoKrates run the following:
export PATH=$PATH:/home/pms/.zokrates/bin
pms@LAPTOP-RNATB7H7:~$ zokartes --version
zokartes: command not found
pms@LAPTOP-RNATB7H7:~$ zokrates --version
zokrates: command not found
pms@LAPTOP-RNATB7H7:~$ export PATH=$PATH:/home/pms/.zokrates/bin
pms@LAPTOP-RNATB7H7:~$ zokrates --version
ZoKrates 0.8.8
```

Compilation stage

```
pms@LAPTOP-RNATB7H7:~$ ls
input.txt  sha256.zok
pms@LAPTOP-RNATB7H7:~$ zokrates compile -i sha256.zok
Compiling sha256.zok

Compiled code written to 'out'
Number of constraints: 48886
pms@LAPTOP-RNATB7H7:~$ ls
abi.json  input.txt  out  out.r1cs  sha256.zok
```

Setup phase where compiled code is used to generate proving & verification keys.

```
pms@LAPTOP-RNATB7H7:~$ zokrates compute-witness -a 0 0 0 1129529685 285551088474675990519063
903894825317322 192916772619636604765586326883831074249
Computing witness...
Witness file written to 'witness'
pms@LAPTOP-RNATB7H7:~$ ls
abi.json  out          out.wtns      sha256.zok      witness
input.txt out.r1cs      proving.key    verification.key
pms@LAPTOP-RNATB7H7:~$ zokrates generate-proof
Generating proof...
Proof written to 'proof.json'
pms@LAPTOP-RNATB7H7:~$
```

```
Performing verification...
PASSED
```