

could we cover some basics of recursive snarks ?

yes, we are going to cover recursive snarks

Fox Reymann | 02/09/2023

do any big projects actually use zocrates? or is it more of a hobby/educational/small project tool?

small project, I don't know of any big projects using Zokrates

Fox Reymann | 02/09/2023

Do we need to submit the homeworks to pass the bootcamp?

No but you will need to contribute to the group homework sessions.

Moderator | 02/06/2023

Do you need a different verifier solidity code for each witness?

no

Fox Reymann | 02/09/2023

does the witness always fall under private input ?

yes

Moderator | 02/10/2023

Does zocrates compile to solidity or directly to EVM bytecode

zokrates compiles to an arithmetic circuit

Fox Reymann | 02/09/2023

Does Zokrates tool also allow to export the program that provers will use to generate Proofs

the program is public, it is not re creatable from the keys though

Moderator | 02/10/2023

For NP-Complete problems, if you find out an initial answer, are the rest of the problems findable in polynomial time or lower?

yes, you can solve other answers in polynomial time

Fox Reymann | 02/09/2023

For the first question in the homework, do we find the additive inverse or multiplicative inverse ?

multiplicative

Moderator | 02/09/2023

how did you call Verifyx() with one parameter yet it takes 2 params?

it uses an array

Moderator | 02/10/2023

How do the Pasta curves in Halo2 help make a zkSNARK setup trustless?

I will explain in a future lesson

Moderator | 02/09/2023

How much does being a smart contract dev will help for this course?

A lot. We talk about ZKP being used mostly for scaling smart contract blockchains.

Fox Reymann | 02/06/2023

How often does the trusted setup need to be done ?

Can we reuse an existing trusted setup for other new systems ?

once per SNARK based ZKP system setup. Can we reuse? That wouldn't be safe.

Fox Reymann | 02/09/2023

In the Polynomials in ZKPs, is the information that the Prover is trying to Prove the fact that they know what the Verifier's

polynomial is?

good shot! but not exactly. the prover is trying to prove that he knows a specific value, we can encode this is a polynomial.

Fox Reymann | 02/09/2023

Interested to learn more about possible use of HE algorithms that can handle floating numbers in non expensive manner

i will investigate

Moderator | 02/10/2023

is kzg ceremony similar to that.

yes, it is also a mpc

Moderator | 02/10/2023

Knowledge of lambda doesn't give away w, but it can trick the verifier into thinking that they do?

yes , knowledge of lambda allows someone to create false proofs and have them accepted by the verifier

Moderator | 02/10/2023

please explain trusted setups with an example

stay tuned, we will

Fox Reymann | 02/09/2023

since we are using Modular Arithmetic, isn't it true that we will find a set of x and y for given $E(x, y)$?


yes

Moderator | 02/10/2023

So why would trusted setups be bad? If you can get enough people, the chance to collusion can basically be zero.

systems without trusted setups are better. trusted setup is a necessity for SNAKRs

Fox Reymann | 02/09/2023

what is  that Victor (Verifier) using here?

public input

Fox Reymann | 02/09/2023

What is a trusted setup? Could they alternatively use a distributed setup like the zkg ceremony?

we are going to explain trusted setup in details

Fox Reymann | 02/09/2023

What is an HH or HE algorithm ?

Homomorphic Hiding and Homomorphic Encryption

Fox Reymann | 02/09/2023

What is N here in SNARKs prover complexity ?

a measure of the size / complexity of the program

Moderator | 02/10/2023

What's the difference between poly-log(N) and log(N)?

logarithmic time $T(n) = O(\log(n))$

polylogarithmic time $T(n) = O(\log(n)^k)$

Fox Reymann | 02/09/2023

Where does pk and vk come from? Are they outputted from C or are they unrelated?

they come from key generation algorithm. Yes, based on C

Fox Reymann | 02/09/2023

why does the ceremony take 2 weeks ? is the proving time itself long ? or is that the window set to let multiple parties to contribute to the ceremony ?

for multiple parties to contribute, computation doesn't take 2 weeks

Fox Reymann | 02/09/2023

Will $E(x+y) = E(x) + E(y)$?

possible

Fox Reymann | 02/09/2023

Will we learn how to use ZK proof to create confidential applications ?like tornado cash or decentralized identity for example ?

You are going to learn all the theory needed and get some practise.

Fox Reymann | 02/06/2023