CS491/492 Weekly Log

2024/2025 Bilkent

Emrehan Ateş

22003465

IAWIA

T2424

11/11/2024

This week I implemented the static web page for the project website. I added the logbook, deliverables and repo link into it. I also linked the webpage to the domain name we bought (iawia.xyz).

20/11/2024

I worked on the specification document this week. The Merkle Tree that we will use to create commitments needed to be decided. I did academic research on different Merkle Tree implementations and found a fitting one to our project. We will use the Lean IMT implementation. We also talked about the design constraints and tech stack of our project as a group.

27/11/2024

This week we gathered as a group after the seminar. We spoke about Vitalik Buterin's new paper about ideal wallets. We thought that our IAWIA could be a way to implement wallets with uniqueness support since passports are unique to beholder. We also brainstormed on using the passport and maybe some other attributes to hide the private key in a secure way. There might be some problems to tackle in this aspect though. For example, we might create cryptographic commitments using those attributes to get the private key back when needed (Shameer's algorithm looks like a fitting solution), however where are we going to store those commitments. If we store them on blockchain there will be up there forever and even though they are hashes, some strong algorithms may be invented in the future to crack them.

03/12/2024

This week we needed to deliver the analysis and requirements report. I worked on the use case part. Our project does not have a long list of scenarios. We only have a few pages on the frontend and no backend. This may seem like we have a small project to implement, but the technicality of the project still scares me. We will need a way to run the circuits on device or on chain.

10/12/2024

I worked on the zero-knowledge concept, mainly on set theory and group theory. Finally, I found a good resource on zero-knowledge on the internet (it is really not easy to find a sufficient and broad one). I examined a few NP problems and their corresponding arithmetic circuits. I think I will take an abstract algebra course from the math department next semester, just to get myself more familiarized with the ZK concept.

17/12/2024

Demo is the upcoming challenge. Serhat is responsible for the frontend side which is his forte and me and Eren are working on the ZK. We need to get ourselves familiarized with the ceremony of tau and snarks. We are building circuits to check the user's age and passport’s expiration date. It would be cool to check the validity of the e-passport but there is a problem on that topic.

Passports have a CSC (country signer) and a DSC (document signer), one public key(PK) checks if it is given by that country and other PK checks if the signature on the passport is valid. Turkey’s CSC is on the International Civil Aviation Organization’s masterlist but its DSC is not. I currently do not have a solution to this, but there are several apps on mobile (e.g. ReadID Me) which successfully checked the validity and CSC-DSC pair of my passport. We might contact the developers of those apps to ask how they achieved this.