CNS Term Project Proposal

A Deep Dive Into Anonymous Authentication System With Zero-Knowledge Proof

R08922161
M10915072
B08902124
B05901044

1 MOTIVATION

Since more and more people have got COVID-19 vaccine, the idea of vaccine certificate system is mentioned in many place, which is said to help people travel across country border easier. Although building such a large system seems to be hard, we might expect the idea would be adopted in smaller scale such as getting into workspace or theater without lining up taking temperature in the near future.

However, in such use case, there is a main drawback that when we are proving our ownership of a vaccine certificate, we might leak our personal information to the verifier or the system, which is undesired invasion of privacy. So we are wondering how to achieve a system able to authenticate that an user is in a membership set without revealing his identity, which is also known as **Anonymous Authentication System**. Then we found Zero-Knowledge Proof might be the most important block to build such a system, which allows us prove the possess of knowledge without revealing it.

Fortunately, ZKP is getting pratical for general programing since [GGPR13] and developer freindly with many tools showing up. So it might be worthwhile to not only do the research of such system but also try to implement one with modern tools.

2 PLAN

To have a better understanding of current state of research about anonymous authentication system, we will first do a comprehensive research on it to check what's the possible solution to build such a system and what's the main challenges we are facing.

In the meantime, we are going to understand how the state-of-art ZKP system [Gro16] works and try to build programmable ZKP above it with Circom, which is a programming language that allows us to build general program in ZKP easily.

Finally, we expect to implement an anonymous authentication system with ZKP and then build a vaccine certificate system above it to show how it might help in real world situation.

3 TIMELINE

We are going to have a checkpoint per week, and here is our goal to check in each checkpoint:

(1) **05/11** - Having understanding about current solutions and problems about anonymous authenticate system.
(2) **05/18** - Having understanding about how [Gro16] works and able to build general program in Circom.
(3) **05/25** - Finish the specification of the anonymous authenticate system and vaccine certificate system we are going to build.
(4) **06/01** - Finish anonymous authenticate system.
(5) **06/08** - Finish vaccine certificate system and TUI client to interact with it.

4 DELIVERABLES

In the end of this term project, we expect to deliver:

- A research report about anonymous authentication system
- A proof-of-concept anonymous authentication system built with ZK-SNARK

REFERENCES

[GGPR13] R. Gennaro, C. Gentry, B. Parno, and M. Raykova. Quadratic span programs and succinct nizks without pcps. In *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, pages 626–645, 2013.

[Gro16] J. Groth. On the size of pairing-based non-interactive arguments. In *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II*, pages 305–326, 2016.