ZKAV:Zero Knowledge proof for AV

Presenting author

Heera G. Wali, Vishal Kulkarni , Rajashekar Ganiger , Nalini C. Iyer

heerawali@kletech.ac.in, nalinic@kletech.ac.in

Abstract

- This study investigates how blockchain technology can be used in the automotive industry and society, with a focus on addressing privacy concerns and compliance issues.
- the application of privacy-preserving methods, including zero knowledge proofs and anonymous credentials, to protect vehicle data shared with servers and prevent V2X channel spam

Zero Knowledge Proofs

- Zero-knowledge proofs are cryptography protocols that allow one party (the prover) to prove to another party (the verifier) that a statement is true without revealing any specific information

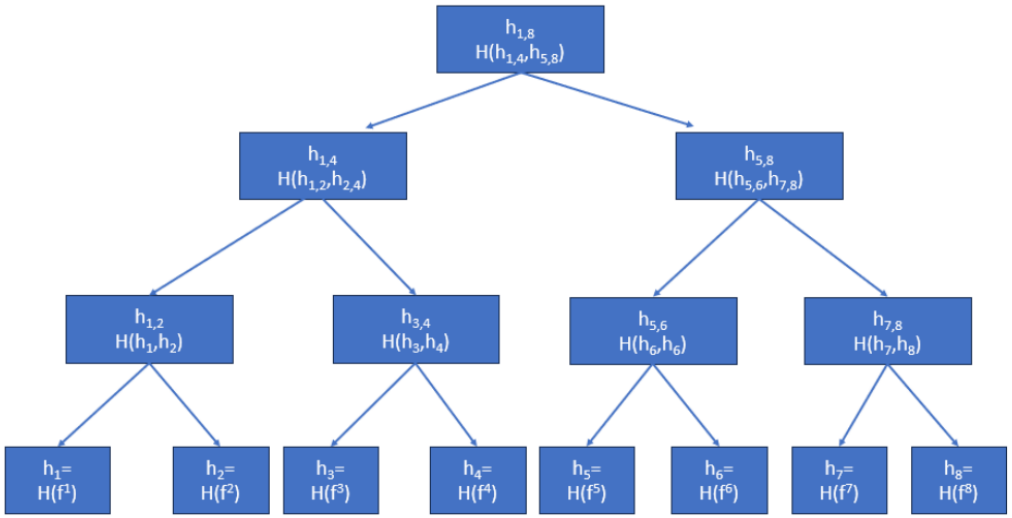
- Completeness
  - If the statement being proven is true, a honest prover can convince the verifier of its truth.

- Soundness
  - If the statement is false, no cheating prover can convince the verifier otherwise

- Zero-Knowledge Property
  - zk-STARKs and zk-SNARKs are the most compelling zero-knowledge technologies in the market today
  - zk-STARK stands for zero-knowledge scalable transparent argument of knowledge, and zk-SNARK stands for zero-knowledge succinct non-interactive argument of knowledge

Merkle tree

- Merkle tree is a binary tree structure commonly used in cryptography and data verification
- It is constructed by hashing data in leaf nodes, then hashing pairs of leaf hashes to create parent node hashes, and repeating until a single root hash is obtained this root hash represents the entire dataset's integrity



Merkle tree

Shamir’s Secret Sharing Scheme

- it allows you to split this secret into n parts (each individual part doesn’t give any information about the secret) and restore this secret upon presentation of k (k¡=n) parts
- for example, you have a secret that you want to split into n parts/shares you can divide these shares between your friends (1 share to 1 friend) now when k of your friends reveal their share, you can restore the secret this scheme is also called (k,n) threshold secret sharing

Rate Limiting Nullifier

- RLN is a zero-knowledge gadget that enables spam prevention in anonymous vehicle environments the anonymity property opens up the possibility for spam, which could seriously cause many security, data manipulation and the overall functioning of the V2X.
- Consider a chat application where users are anonymous now, everyone can write an unlimited number of spam messages, but we don’t have the ability to kick this member because the spammer is anonymous RLN helps us identify and ”kick” the spammer there are also ’nullifier’ and ’external nullifier’, which can be found in the RLN protocol/circuits,

How RLN works?

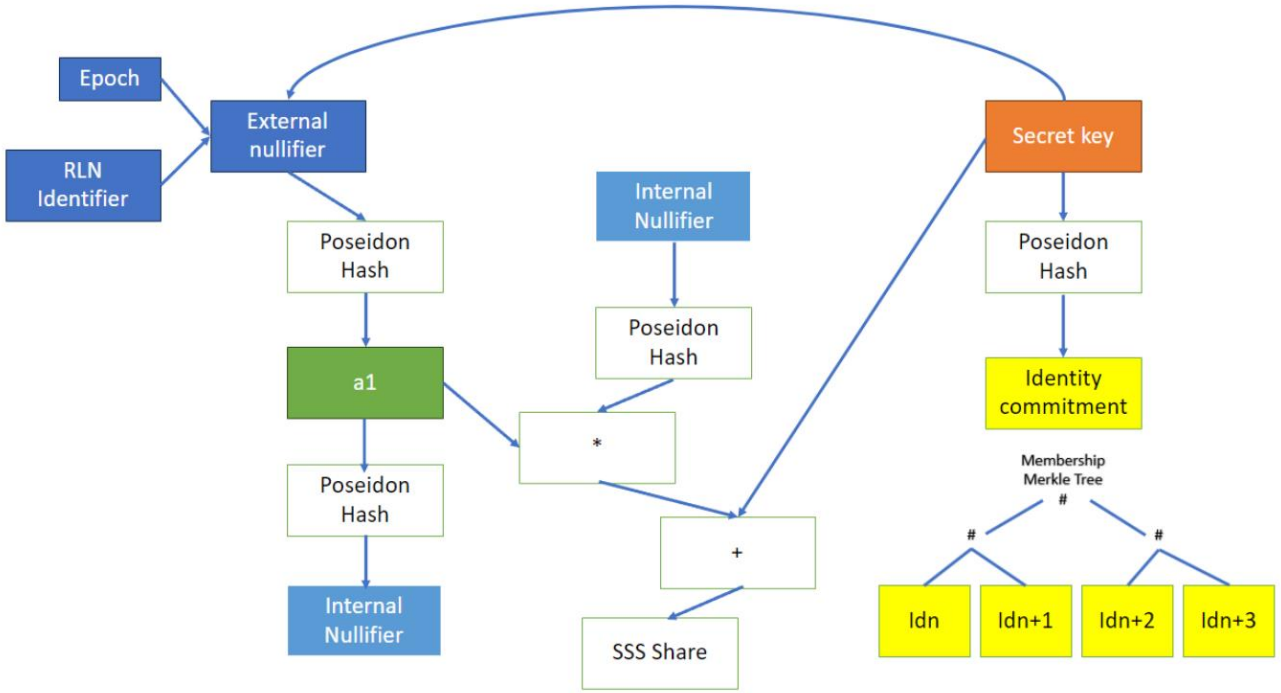
- The RLN construct functionality consists of three parts
  - Registration
  - Interaction
  - Slashing

- Registration
  - the user registers to the application by providing a form of stake vehicle needs to create a Merkle tree, and every participant must submit an identity commitment and place it in the Merkle tree

- Interaction
  - each interaction that the vehicle wants to make with the application, the vehicle must generate a zero-knowledge proof ensuring that their identity commitment (or specifically rate commitment) is the part of the membership Merkle tree

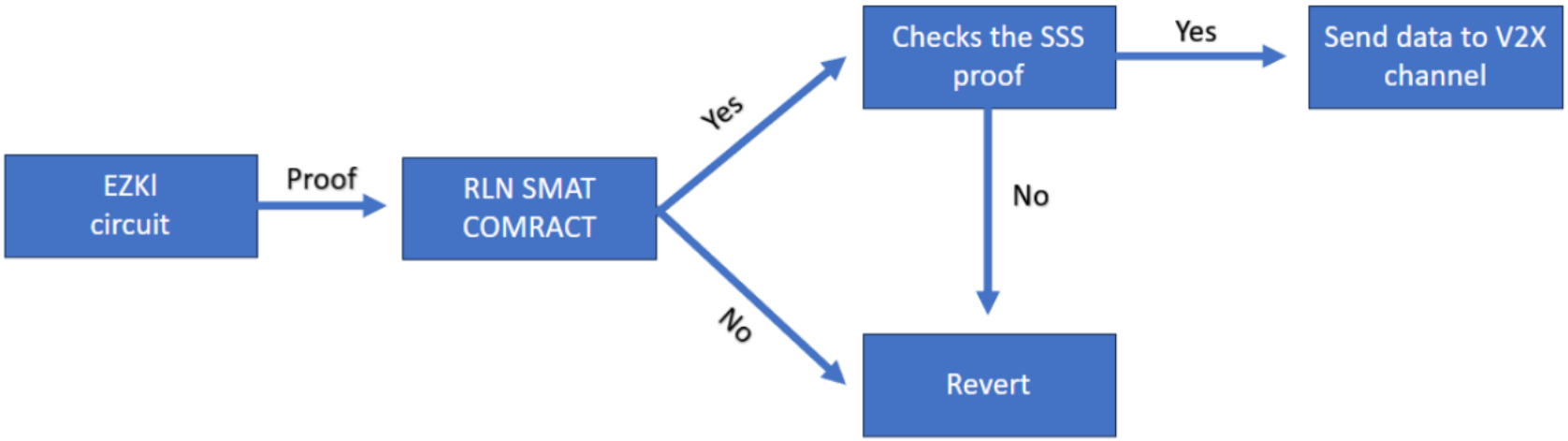
- Slashing
  - it allows for the users to be removed from the membership tree by anyone that knows their secret key thus, if someone spams, it'll be possible to recover the secret key and withdraw the stake of a spammer

RLN circom circuit



RLN circom circuit

model for ZKAV



. Proposed model for ZKAV

Conclusion

- it enables the creation of proofs for various applications such as object detection and number plate recognition
- RLN (Ring Learning Network) circuits developed using the circom DSL (Domain Specific Language), which serves as a robust spam protection mechanism for V2X
- this innovative system combines machine learning, blockchain technology, and cryptographic protocols to create a secure and verifiable environment for applications like object detection and V2X communication it bridges the gap between AI model outputs and secure data transmission, ensuring the integrity of information in emerging digital ecosystems.

Limitations

- The limitations of this project arise from the choice of using ethereum, a public block chain, for automotive vehicles although private blockchains are better suited for automotive applications
- Ethereum smart contracts requires significant computational resources, which could overload the vehicle’s computing capacity
- the project faces limitations due to its reliance on ethereum and the computational burden it places on automotive vehicles, necessitating a focus on computational capacity improvements

iSCSi 2023 official Sponsors

Platinum

Gold

Silver

Institutional