ZKU - Assignment 5


```
Email - stanleychiu@protonmail.com
Discord - HKerStanley#4125
GitHub - https://github.com/HKerStanley/zk-uni (./asset/week_5)
```


Question 1: Shielding the TX

1. Such protocol would be a combined version of a mixer and cross-chain bridge. User will be able to deposit tokens on one side, for example Ethereum, and generate a zero knowledge proof for the ownership of fund. The smart contract will update the Merkle Tree to commit the new Merkle root after deposit. This new Merkle root then should be relayed to the other side of bridge, for example Harmony, so that the state of the mixer will be synchronized on both chain. User will then be able prove to the protocol with the zero knowledge proof generated when deposit, that they own certain amount of tokens in the protocol. One major challenge here is how to garantee state of protocol is synchronized on both blockchain. Imagine a situation that a user make a withdrawal on both blockchain at the same time, it might cause a double spending situation on both chain and that user will be able to generate fund from nothing. To prevent this happen, the protocol can add an extra layer during the withdrawal that lock up fund on the other chain. Briefly speaking when a user try to withdraw tokens on Ethereum, a signal will send to Harmony to lock the state until the withdrawal finished and a new state is committed on chain.

2. The Wormhole hack is based on a signature verification vulnerability so that the hacker is able to mint token on Solana without a valid signature. To prevent this happen I think I would use the similar approach as mentioned above. The verification process should also include a lock which temporary hold up fund on both chains, and make sure the state of both sides are synchronized before any execution especially for withdrawal.

Question 2: Aztec

1. AZTEC note is a encrypted representation of abstract value. It is comprised of a tuple of elliptic curve commitments and 3 scalars: a viewing key, a spending key and a message. The message can be the representation of various assets. The viewing key and spending key are used to create valid join-split transaction proof and allow the AZTEC note be decrypted, revealing the message.
    - Range proofs: It is used to prove an AZTEC note is greater/smaller than a public integer, so can be used to prove that ownership of an asset after a trade is within a regulatory range.
    - Swap proofs: It is a proof of atomic swap of 2 AZTEC notes. It is useful for trading assets by proving the makers bid note equal to takers ask note.
    - Dividend proofs: It is a proof of the input AZTEC note equals to an output AZTEC notes multiplied by a ratio. It can be used for paying interest from asset.
    - Join-split proofs: It is a proof allows a set of input notes to be joined or splited into a set of output notes. It ensures the sum of input equals to the sum of output so can be used in asset transaction given that AZTEC protocol follows UTXO model and transactions can consist different size of notes and number of join/split process.

Question 3: Webb

1. Anchor commitment is more similar to what Tornado Cash do, to support a fixed amount but added a destinated chain id in the commitment. While VAnchor is more similar to Tornado Nova, the commitment takes an amount variable so can be used for UTXO join/split transaction. I think we can add a liquidity token id parameter to the commitment structure so it can represent a token swap pair. The commitment will look like `commitment = Poseidon(chainID, amount, pairID, pubKey, blinding)` where `pairID` is the trading pair, for example `ETHBTC` which implies users' stake of a liquidity pool, and being able to withdraw 2 types of token.

2. Anchor's commitment has destinated chain id to support cross-chain bridge function.

3. Token are stored in the Merkle Tree following the UTXO model, where users are required to create and deposits UTXOs. The sum of UTXOs amount have to equal to the deposit amount. The UTXOs will become the commitment hash input and generate zkSnark proof and will be verified by the contract. They will be located in one-of-many VAnchor Merkle trees and the chain id should match both commitment and the VAnchor Merkle Tree.

Question 4: Thinking In ZK

1. Is there any chance Webb protocol can leverage the AZTEC protocol? With the suport of AZTEC note I think Webb can achieve a lot of exciting features as a private bridge.

Question 5: Final Project

Link to my proposal: https://github.com/HKerStanley/zk-uni/blob/main/asset/week_5/final_project_proposal.pdf