Homework 12

> ## Using Circom REPL
>
> See this partial circom code
>
> Using this code in the zkREPL, complete the constraint on line 19 and add some appropriate inputs in the input section.
> Test that it creates a proof, and show that an incorrect proof fails.

Team Discussion

Imagine you are developing a project and want to use one of the zkRollup based L2s.
1. What factors would be important to you when choosing which to use.
2. Of the protocols we have seen so far, which would you choose ?
2. The Mina - ETH bridge uses a STARK to prove the verification of a SNARK proof, what could be the rational behind mixing these 2 types of proving systems ?

1) When choosing between different Layer 2 (L2) zk-rollup solutions, key factors to consider include security, scalability, cost, interoperability, user experience, ecosystem support, upgradeability, auditing and code quality, token support, and the availability of a token bridge. Prioritize security, scalability, and low costs, while also considering how well the L2 integrates with the broader Ethereum ecosystem and whether it offers a seamless user experience. Additionally, assess its capacity for future upgrades and its support for a variety of tokens and assets.

2) My top L2 rollup choice would be StarkNet due to its high security, scalability, and Ethereum ecosystem integration.

3) Pros of mixing zk-SNARKs and STARKs: Enhanced security, scalability, diversification of risk.

Cons: Complexity, interoperability challenges, higher development overhead, potential for increased gas costs, unproven integrations.