Hello everyone,

I’m reaching out with a specific question regarding ZKP in the context of generating an ECDH secret share using Ethereum keys.

My goal is to determine if it is possible to prove, within a ZKP circuit, that an ECDH secret share is correctly generated using an Ethereum private key and an Ethereum public key.

Here are the potentials specifics input:

1. Public Inputs:
2. Two EVM addresses (keccak256 hash of Ethereum public keys).
3. Private Input:
4. An Ethereum private key.

My questions are as follows:

- Is it technically feasible to use these values (private key and public key) within a plonk circuit?
- Is it possible to construct a ZKP to prove the correct generation of the ECDH secret share?

Thank you in advance for your assistance and contributions!

Shuffle