This is a request for review of sparse merkle tree membership check using using dalek’s Bulleptoofs implementation. There are some working tests.

I have 2 variations of the naive sparse mekle tree as described here, binary and 4-ary.

Implementation of the naive binary sparse merkle tree and its constraints.

Implementation of the naive 4-ary sparse merkle tree and its constraints.

I am using the Poseidon hash function. There are 2 variations of it, one that hashes 2 inputs in a call and another hashes 4 inputs in a single call. I use the former for binary tree and latter for 4-ary tree.

I am more interested in the review of sparse merkle tree constraints.

I have an optimized sparse merkle tree implementation but in that merkle proof are of variable number of nodes hence the proof size of Bulletproofs will change which might give the verifier an idea of where the leaf is in the tree. Is there an alternate approach?