LeanIMT: An optimized IMT

Privacy & Scaling Explorations

June 4, 2024

1 Abstract

Contents

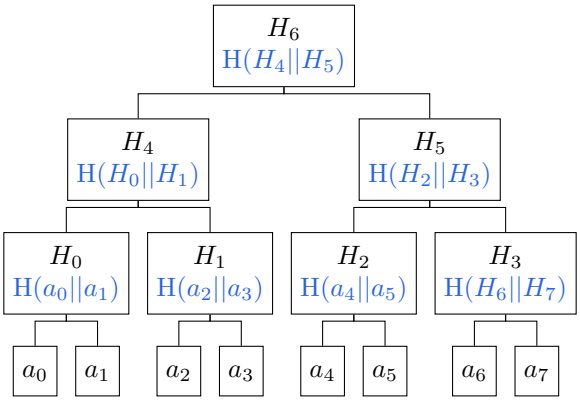
2 Introduction

2.1 Motivation

3 Merkle Tree

3.1 Incremental Merkle Tree

TODO: Explain what is a Merkle tree and an Incremental Merkle Tree.

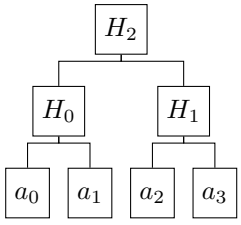


4 LeanIMT

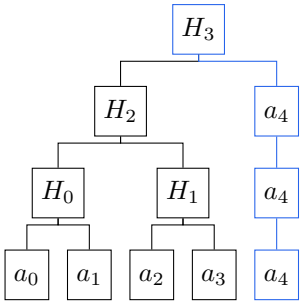
$T = (V, E)$

$V = \{a_0, a_1, a_2, a_3, H_0, H_1, H_2\}$

$E = \{(a_0, H_0), (a_1, H_0), (a_2, H_1), (a_3, H_1), (H_0, H_2), (H_1, H_2)\}$



Before inserting a_4



After inserting a_4

5 Benchmarks

6 Conslusions

This document is based on the work of [1].

References

[1] Barry Whitehat Kobi Gurkan Koh Wei Jie. "Semaphore: Zero-Knowledge Signaling on Ethereum". In: (2020). URL: https://semaphore.pse.dev/whitepaper-v1.pdf.