

LeanIMT: An optimized IMT

Privacy & Scaling Explorations

June 5, 2024

1 Abstract

Contents

1	Abstract	1
2	Introduction	3
2.1	Motivation	3
3	Merkle Tree	3
3.1	Incremental Merkle Tree	3
3.2	Binary Tree	3
4	LeanIMT	3
4.1	Definition	3
4.2	Insertion	4
5	Benchmarks	4
6	Conslusions	4

2 Introduction

2.1 Motivation

3 Merkle Tree

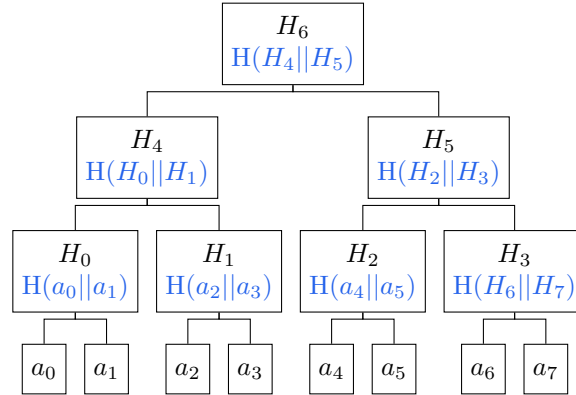
3.1 Incremental Merkle Tree

An Incremental Merkle Tree (IMT) is a Merkle Tree (MT) designed to be updated efficiently.

3.2 Binary Tree

A Binary Tree is a tree data structure in which each node has at most two children, referred to as the left child and the right child.

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



4 LeanIMT

4.1 Definition

The **LeanIMT** (Lean Incremental Merkle Tree) is a Binary IMT.

The LeanIMT has two properties:

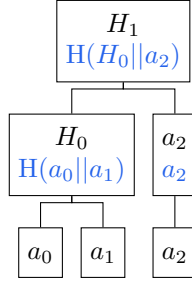
1. Every node with two children is the hash of its two child nodes.
2. Every node with one child has the same value as its child node.

Example of a LeanIMT

$$T = (V, E)$$

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

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

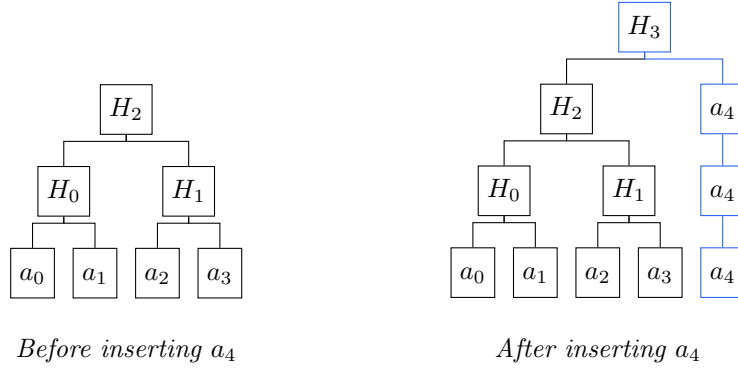


4.2 Insertion

$$T = (V, E)$$

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

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



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>.