24.12.03 Merkle Path with Different Opening Number

Xun Zhang   Wuyun Siqin   Bingsheng Zhang

Zhejiang University, CHN

22221024@zju.edu.cn   3210101763@zju.edu.cn   bingsheng@zju.edu.cn

December 3 2024

1 Merkle Path with Selector

We have benchmarked the Merkle path circuit with selector, and the opening number of Merkle tree is half of total leaf nodes.

This time we benchmarked various numbers of opening nodes, the results is like following:

degree	num_aggregation	num_origin	proof_time	proof_size	verify_time
19	64	1024	17.9436s	2816	8.5181ms
19	128	1024	29.7951s	4928	8.4833ms
19	256	1024	56.6890s	9152	10.1941ms
19	512	1024	103.6901s	17600	13.5464ms
19	768	1024	162.6483s	26048	36.4137ms

Table 1: Merkle Tree Path 1024 Benchmark

degree	num_aggregation	num_origin	proof_time	proof_size	verify_time
19	128	2048	44.2524s	5280	8.9935ms
19	256	2048	61.4681s	9856	10.9770ms
19	512	2048	113.1540s	19360	15.5076ms
19	1024	2048	222.6445s	38016	24.4505ms
19	1536	2048	328.6864s	56672	34.4368ms

Table 2: Merkle Tree Path 2048 Benchmark

Note that this circuit does not include the constraints of index, so the actual proving will be longer than results in the table.

degree	num_aggregation	num_origin	proof_time	proof_size	verify_time
19	256	4096	60.8389s	10560	44.3780ms
19	512	4096	115.4392s	20768	14.6929ms
19	1024	4096	234.0109s	40832	22.1103ms
19	2048	4096	459.3131s	81312	35.0787ms
19	3072	4096	692.4101s	121792	51.12153ms

Table 3: Merkle Tree Path 4096 Benchmark