24.11.19 Merkle Tree Opening Benchmark

Xun Zhang Wuyun Siqin Bingsheng Zhang
Zhejiang University, CHN
22221024@zju.edu.cn 3210101763@zju.edu.cn bingsheng@zju.edu.cn

November 19 2024

1 Merkle Tree Root Benchmark

We implemented the whole Merkle tree root circuit, that is, given a vector of members, proving the Merkle tree root is correctly computed by all the leaf nodes(members).

degree	**num**	**proof_time**	**proof_size**	**verify_time**
19	32	5.9280s	704	5.8417ms
19	64	7.8385s	1056	4.8113ms
19	128	9.7901s	1408	10.0684ms
19	256	13.9924s	2112	7.8568ms
19	512	22.4310s	3520	9.3348ms
19	1024	40.6768s	6688	8.6423ms
19	2048	77.2907s	13024	11.2679ms
19	4096	147.1965s	25344	17.7845ms

Table 1: Merkle Tree Root Benchmark

We also list the benchmark results of the normal opening method of Merkle tree(by providing Merkle tree path).

degree	**num_aggregation**	**num_origin**	**proof_time**	**proof_size**	**verify_time**
19	16	32	5.6890s	704	6.5756ms
19	32	64	7.6071s	1056	4.4714ms
19	64	128	13.4401s	2112	7.6402ms
19	128	256	23.2960s	3872	8.1395ms
19	256	512	48.6304s	8448	11.6570ms
19	512	1024	100.0534s	17600	13.6171ms
19	1024	2048	213.2567s	38016	20.3142ms

Table 2: Merkle Tree Path Benchmark with stake

2 Shuffle Argument in Halo2

We also benchmark the shuffle argument in the halo2, this circuit is the official imlpementation of shuffling.

degree	**vector_length**	**tuple_length**	**proof_time**	**proof_size**	**verify_time**
14	1024	2	0.3576s	608	4.7292ms
15	1024	2	0.6210s	608	4.7848ms
14	2048	2	1.1507s	608	5.0151ms
15	2048	2	1.9449s	608	6.9806ms
14	4096	2	1.1578s	608	6.3846ms
15	2048	2	2.1004s	608	5.5532ms
14	1024	3	1.3217s	736	4.9721ms
15	1024	3	2.1634s	736	5.0851ms
14	2048	3	1.3509s	736	10.3736ms
15	2048	3	2.3449s	736	6.6278ms
14	4096	3	1.3925s	736	6.6628ms
15	4096	3	2.4891s	736	7.0279ms

Table 3: Shuffle Benchmark

Where vector_length is the length of the set we want to prove the relations, and the tuple_length is the length of a tuple in the set.

For example, the length of tuple (pk_i, stake_i) is 2.

Note that when the vector_length is biggner than 1024, the program will meet a stack overflow in the layouter.assign_region function. Add RUST_MIN_STACK=16777216 before your command to solve it.