RISC Zero Datasheet

(April 2023 -- as of commit cd1a37e)

Use cargo run —release —example loop in head of main to collect data for your machine

Metal on M1 MacBook

Cycles	Prover Time	RAM	Proof Size	Speed
32 k	1.38 s	234.4 MB	201.3 kB	23.7 kHz
64 k	1.87 s	468.7 MB	213 kB	35 kHz
128 k	2.80 s	937.4 MB	236 kB	46.9 kHz
256 k	4.97 s	1.87 GB	247.7 kB	52.7 kHz
512 k	9.49 s	3.75 GB	259.9 kB	55.3 kHz
1024 k	17.96 s	7.5 GB	273.2 kB	58.4 kHz
2048 k	50.13 s	15 GB	297.8 kB	41.8 kHz
4096 k	1:51.2	30 GB	311.1 kB	37.7 kHz

Metal on M2 MacBook

Cycles	Prover Time	RAM	Proof Size	Speed
32 k	1.17 s	234.4 MB	201.3 kB	28.1 kHz
64 k	1.49 s	468.7 MB	213 kB	44.1 kHz
128 k	2.06 s	937.4 MB	236 kB	63.7 kHz
256 k	3.39 s	1.87 GB	247.7 kB	77.3 kHz
512 k	6.07 s	3.75 GB	259.9 kB	86.4 kHz
1024 k	11.50 s	7.5 GB	273.2 kB	91.2 kHz
2048 k	21.21 s	15 GB	297.8 kB	98.9 kHz

M1 MacBook - CPU Only

Cycles	Prover Time	RAM	Proof Size	Speed
32 k	2.84 s	234.4 MB	201.3 kB	11.5 kHz
64 k	4.75 s	468.7 MB	213 kB	13.8 kHz
128 k	8.43 s	937.4 MB	236 kB	15.5 kHz
256 k	16.98 s	1.87 GB	247.7 kB	15.4 kHz
512 k	34.65 s	3.75 GB	259.9 kB	15.1 kHz
1024 k	1:22.1	7.5 GB	273.2 kB	12.8 kHz
2048 k	2:20.4	15 GB	297.8 kB	14.9 kHz
4096 k	5:39.8	30 GB	311.1 kB	12.3 kHz
8192 k	14:13.7	77 GB	325 kB	9.8 kHz

AMD Ryzen Threadripper PRO 3995WX 64-Cores

Cycles	Prover Time	RAM	Proof Size	Speed
32 k	1.25 s	234.4 MB	201.3 kB	26.1 kHz
64 k	2.25 s	468.7 MB	213 kB	29.2 kHz
128 k	3.88 s	937.4 MB	236 kB	33.8 kHz
256 k	7.12 s	1.87 GB	247.7 kB	36.8 kHz
512 k	13.81 s	3.75 GB	259.9 kB	38 kHz
1024 k	25.03 s	7.5 GB	273.2 kB	41.9 kHz
2048 k	50.96 s	15 GB	297.8 kB	41.2 kHz
4096 k	1:38.5	30 GB	311.1 kB	42.6 kHz

CUDA on NVIDIA RTX A4000

Cycles	Prover Time	RAM	Proof Size	Speed
32 k	0.87 s	234.4 MB	201.3 kB	37.5 kHz
64 k	1.29 s	468.7 MB	213 kB	50.6 kHz
128 k	2.34 s	937.4 MB	236 kB	56 kHz
256 k	4.20 s	1.87 GB	247.7 kB	62.4 kHz
512 k	7.47 s	3.75 GB	259.9 kB	70.1 kHz
1024 k	13.8 s	7.5 GB	273.2 kB	76 kHz
2048 k	29.81 s	15 GB	297.8 kB	70.3 kHz
4096 k	1:05.6	30 GB	311.1 kB	63.9 kHz

CUDA on NVIDIA RTX A5000

Cycles	Prover Time	RAM	Proof Size	Speed
32 k	0.72 s	234.4 MB	201.3 kB	45.8 kHz
64 k	1.15 s	468.7 MB	213 kB	57 kHz
128 k	1.94 s	937.4 MB	236 kB	67.5 kHz
256 k	3.67 s	1.87 GB	247.7 kB	71.5 kHz
512 k	6.79 s	3.75 GB	259.9 kB	77.2 kHz
1024 k	12.82 s	7.5 GB	273.2 kB	81.8 kHz
2048 k	25.05 s	15 GB	297.8 kB	83.7 kHz
4096 k	58.31 s	30 GB	311.1 kB	71.9 kHz

CUDA on NVIDIA RTX 3090 Ti

Cycles	Prover Time	RAM	Proof Size	Speed
32 k	0.68 s	234.4 MB	201.3 kB	48.2 kHz
64 k	1.08 s	468.7 MB	213 kB	60.7 kHz
128 k	1.80 s	937.4 MB	236 kB	72.8 kHz
256 k	3.39 s	1.87 GB	247.7 kB	77.3 kHz
512 k	6.01 s	3.75 GB	259.9 kB	87.3 kHz
1024 k	11.43 s	7.5 GB	273.2 kB	91.7 kHz
2048 k	22.53 s	15 GB	297.8 kB	93.1 kHz
4096 k	57.11 s	30 GB	311.1 kB	73.4 kHz

Example	Cycles
Factors	32 k
Chess	256 k
Digital Signature	64 k
EVM	2048 k
JSON	64 k
Password Checker	64 k
SHA	64 k
Waldo	8192 k
Wordle	64 k

The performance of the prover depends on the number of execution cycles in the zkVM guest. We therefore give performance data for different guest execution lengths, as indicated in the "Cycles" column. For cryptographic reasons, the cycle count is always rounded up in length to the next highest power of two; thus, a program that requires 33000 cycles will have the same performance as a program that requires 63000 cycles, as both will round up to 65536 (64 k) cycles.

Initializing a zkVM guest requires over 16 k cycles. Combined with this power of two rounding, this means that no program can be executed in fewer than 32 k cycles.

To give context for these numbers we have included a table indicating the size of each of our example programs in cycles. Note that some programs vary in cycle count depending on input data. The cycle counts given here use the default input data, or, for examples with no defaults, the input data suggested in the associated README file.

www.RISCZero.com

zkVM Examples