ZKPwhale Chip技术指标及性能对比

ZKPwhale Chip 主要技术指标

- 支持BLS12-381曲线
- 支持BLS12-377曲线
- 支持BN254曲线
- 支持多标量乘法（Multi-Scalar Multiplication， MSM）
- 支持数论变化（Number Theoretic Transform， NTT）
- 支持长向量模运算
- 支持最大NTT长度：2^27
- 支持最大MSM、 MOD长度：2^30
- 内置2路LPDDR4控制器，最大支持16GB LPDDR4内存
- 内置1路PCIe 16Gbps地从模式设备接口，支持x1、x2、x4链路
- 支持多路GPIO
- 低功耗设计
- 动态芯片温度控制
- 工作温度：-40℃~125℃
- 参数可编程：支持 BN254、 BLS381， BLS377
- 可适配后量子加密、多方安全计算、联邦学习
- MSM 加速 BLS377 2^28 size： 171ms

ZKPwhale Chip性能测试

MSM-Size	Zprize GPU Champion	Ingonyama [1] PipeMSM	Cysic [2] CysicMSM	Accseal Leo Chip	Accseal LeoMSM Board	Accseal LeoMSM Board Pro
	(ms)	(ms)	(ms)	(ms)	(ms)	(ms)
BLS12-377	3090 GPU	FPGA (1x U56C)	FPGA (vu13p)	ASIC芯片 16GB内存，实测数据	ASIC 单算力卡 4芯片，64GB内存，实测数据	ASIC 阵列(8算力卡) 512GB内存，实测数据
2^14				1.16	0.29	0.05
2^16		18		2.20	0.55	0.10
2^18		72		5.20	1.31	0.25
2^20	23	273	50	19	4.9	0.9
2^22	67	1092	196	115	28.9	5.1
2^24	218	4368	780	337	84.4	15.9
2^26	854	17472	3117	1228	307.2	50.2
2^28	3347	69888	12464	4915	1229.1	171.5
算力加速比	0.83	0.07	0.38	1	3.86	20.95
平均功耗（W）	380	115	95	20	95	760
单位算力功耗比	23.00	82.62	12.50	1.00	1.23	1.81
采购单价	12000	34000	7000	1700	6800	54400
单位算力成本比	8.54	287.37	10.84	1.00	1.00	1.53

- 1）将MSM计算数据拆分成多段，多芯片并行计算，更有利于效率提升；
- 2）Leo芯片测试结果是并行计算1000次的平均时间；
- ps：[1] Data from 2022-999-PipeMSM-note,
  [2] Data from Cysic deck on ConferenceZK,Dec.22,2022

ZKPwhale Chip功耗测试

	单芯片（W）	单卡(W)	运算占比
MSM	46	223	35%
NTT	7	28	25%
MOD	6	25	40%
平均功耗	20.25	95.05	100%
最大功耗	46	223	全部运算MSM

- 环境：inte6262 24核CPU*2，31号6卡机，SDK1.0.9，DDR2133M，2^26，0.88V内核电压
- Training完成：单卡18.72W