Benchmarking Groth16 Proving System

Lehigh University
Tal Derei and Ben Aulenbach
October 2022

This serves as a guide for navigating the excel sheets containing the benchmarks. Each **benchmark** (representing each excel sheet) has **colors** (representing the machine each workload was run on), and a **tag** on the upper right side (representing the repository benchmarked).

Benchmarks

* Parameter and Preprocessing Generation

* CPU Proof Generation

* GPU Proof Generation

Colors

* Pink = 28-core Intel(R) Xeon(R) Gold 5120 CPU @ 2.20GHz, NVIDIA P100 (Pascal Architecture) with 12 GB HBM2, 192 GB DDR4 DRAM, 128 GB SSD.
* Purple = 64-core Intel(R) Xeon(R) Platinum 8358 CPU @ 2.60GHz, NVIDIA A10 (Ampere Architecture) with 24 GB GDDR6, 1024 GB DDR4 DRAM, 2 TB SSD.
*Green = NVIDIA A40 (Ampere Architecture) with 48 GB GDDR6.

Tags

FIGURE 1 = snark-challenge-prover-reference repository:
https://github.com/TalDerei/snark-challenge-prover-reference

FIGURE 2 and FIGURE 3 = gpu-groth16-prover-3x:
https://github.com/TalDerei/gpu-groth16-prover-3x

FIGURE 4 = ZPrize (test-msm-gpu): https://github.com/TalDerei/test-msm-gpu

PARAMETER AND PREPROCESSING GENERATION

Parameter Generation Benchmarking — FIGURE 1

snark-challenge-prover-reference repository: https://github.com/TalDerei/snark-challenge-prover-reference

Generating the public parameters (proving and verification keys) and inputs on CPU (there isn't a GPU option)

Execution Time = seconds

Intel(R) Xeon(R) Gold 5120 CPU @ 2.20GHz

CPU Utilization = percent

Core Count: 28 | **Memory (GB): 192 GB** | **Network bandwidth (Gbps): 50** | **Boot Disk: 128 GB** | **Year: Q3 2017**

Memory Utilization = GB

	2^15	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Parameter File Size
		30.33	0		
		30.06	0		
Total:		**30.195**	**0**	**13M**	**37M**

	2^16	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Parameter File Size
		43.47	0.192		
		43.53	0.192		
Total:		**43.5**	**0.192**	**25M**	**73M**

	2^17	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Parameter File Size
		53.39	1.426944		
		53.75	1.425792	**49M**	**145M**
Total:		**53.57**	**1.426368**		

	2^18	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Parameter File Size
		98.93	2.153522765		
		98.34	2.1736512		
Total:		**98.635**	**2.163586982**	**97M**	**289M**

	2^19	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Parameter File Size
		147.74	4.6699008		
		148.33	4.7122944		
Total:		**148.035**	**4.6910976**	**193M**	**577M**

	2^20	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Parameter File Size
		270.99	9.312		
		272.45	9.039017414		
Total:		**271.72**	**9.175508707**	**385M**	**1.2G**

	2^21	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Parameter File Size
		584.49	19.0272		
		581.79	19.2		
Total:		**583.14**	**19.1136**	**769M**	**2.3G**

	2^22	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Parameter File Size
		1115.58	36.9408		
		1113.57	36.8832		
Total:		**1114.575**	**36.912**	**1.6G**	**4.6G**

	2^23	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Parameter File Size
		2016.29	62.4768		
		2014.33	61.92		
Total:		**2015.31**	**62.1984**	**3.1**	**9.1**

	2^24	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Parameter File Size
		3568.72	124.9536		
		3563.53	124.8576		
Total:		**3566.125**	**124.9056**		

	2^25	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Parameter File Size
		Process killed due to insufficient memory (192 GB)			
Total:					

Parameter Generation Benchmarking — FIGURE 2

snark-challenge-prover-reference repository: https://github.com/TalDerei/snark-challenge-prover-reference

Generating the public parameters (proving and verification keys) and inputs on CPU (there isn't a GPU option)

Execution Time = seconds

Intel(R) Xeon(R) Platinum 8358 CPU @ 2.60GHz

CPU Utilization = percent

Core Count: 128 | **Memory (GB): 1024 GB** | **Network bandwidth (Gbps): 50** | **Boot Disk: 128 GB** | **Year: Q2 2021**

Memory Utilization = GB

	2^15	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Parameter File Size
		8.62	0		
		9.16	0		
Total:		**8.89**	**0**	**13M**	**37M**

	2^16	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Parameter File Size
		18.68	0.512		
		18.52	0.512		
Total:		**18.6**	**0.512**	**25M**	**73M**

	2^17	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Parameter File Size
		24.89	1.02		
		25.07	1.02	**49M**	**145M**
Total:		**24.98**	**1.02**		

	2^18	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Parameter File Size
		58.76	2.46		
		58.54	2.46		
Total:		**58.65**	**2.46**	**97M**	**289M**

	2^19	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Parameter File Size
		95.13	4.71		
		95.21	4.81		
Total:		**95.17**	**4.76**	**193M**	**577M**

	2^20	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Parameter File Size
		171.57	8.8		
		172.42	8.91		
Total:		**171.995**	**8.855**	**385M**	**1.2G**

	2^21	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Parameter File Size
		393.23	19.15		
		393.98	19.25		
Total:		**393.605**	**19.2**	**769M**	**2.3G**

	2^22	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Parameter File Size
		761.85	36.86		
		757.56	36.97		
Total:		**759.705**	**36.915**	**1.6G**	**4.6G**

	2^23	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Parameter File Size
		1358.07	61.92		
		1362.01	61.19		
Total:		**1360.04**	**61.555**	**3.1G**	**9.1G**

	2^24	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Parameter File Size
		2231.07	120.52		
		2235.06	120.55		
Total:		**2233.065**	**120.535**	**6.1G**	**19G**

	2^25	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Parameter File Size
		3907.86	240.438		
		3901.12	214.52		
Total:		**3904.49**	**227.479**	**12.2G**	**40G**

Parameter Preprocessing Generation Benchmarking — FIGURE 3

snark-challenge-prover-reference repository: https://github.com/TalDerei/snark-challenge-prover-reference

Generating the public parameters (proving and verification keys) and inputs on CPU (there isn't a GPU option)

Execution Time = seconds

Intel(R) Xeon(R) Platinum 8358 CPU @ 2.60GHz

CPU Utilization = percent

Core Count: 128 | **Memory (GB): 1024 GB** | **Network bandwidth (Gbps): 50** | **Boot Disk: 128 GB** | **Year: Q2 2021**

Memory Utilization = GB

	2^15	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Preprocessing File Size
		34.11	0		
		34.12	0		
Total:		**34.115**	**0**	**13M**	**745M**

	2^16	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Preprocessing File Size
		62.28	1.02		
		62.29	1.02		
Total:		**62.285**	**1.02**	**25M**	**1.5G**

	2^17	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Preprocessing File Size
		104.38	2.46		
		104.32	2.46		
Total:		**104.35**	**2.46**	**49M**	**3.0G**

	2^18	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Preprocessing File Size
		199.55	4.92		
		199.65	4.81		
Total:		**199.6**	**4.865**	**97M**	**5.9G**

	2^19	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Preprocessing File Size
		379.64	9.83		
		378.93	9.83		
Total:		**379.285**	**9.83**	**193M**	**12G**

Parameter Generation Benchmarking — FIGURE 4

ZPrize (test-msm-gpu): https://github.com/TalDerei/test-msm-gpu

Benchmarking ZPrize's MSM parameter generation on CPU (there isn't a GPU option) -- this is not comparable to running a fully complete trusted setup ceremony required by a prover

Intel(R) Xeon(R) Platinum 8358 CPU @ 2.60GHz

Core Count: 128 | **Memory (GB): 1024 GB** | **Network bandwidth (Gbps): 50** | **Boot Disk: 128 GB** | **Year: Q2 2021**

	2^15	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)
		0.051	**Negligible**
		0.046	
Total:		**0.0485**	

	2^16	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)
		0.06	**Negligible**
		0.061	
Total:		**0.0605**	

	2^17	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)
		0.08	**Negligible**
		0.076	
Total:		**0.078**	

	2^18	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)
		0.11	**Negligible**
		0.111	
Total:		**0.1105**	

	2^19	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)
		0.174	**Negligible**
		0.173	
Total:		**0.1735**	

2^20	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Preprocessing File Size
	754.57	20.07		
	755.43	20.17		
Total:	755	20.12	385M	24G

2^21	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Preprocessing File Size
	1499.83	38.71		
	1503.98	38.6		
Total:	1501.91	38.655	769M	47G

2^22	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Preprocessing File Size
	3063.88	78.03		
	3065.65	77.93		
Total:	3064.765	77.98	1.6G	94G

2^23	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Preprocessing File Size
	6142.21	156.04		
	6145.65	156.13		
Total:	6143.93	156.085	3.1G	187G

2^24	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Preprocessing File Size
	11913.42	311.78		
	11917.11	310.26		
Total:	11915.265	311.02	6.1G	373G

2^25	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)	Input File Size	Preprocessing File Size
	23234.77	620.24		
	23239.12	621.42		
Total:	23236.945	620.83	12.2	751G

2^20	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)
	0.316	Neglible
	0.304	
Total:	0.31	

2^21	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)
	0.568	Neglible
	0.563	
Total:	0.566	

2^22	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)
	1.09	Neglible
	1.09	
Total:	1.09	

2^23	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)
	2.02	Neglible
	2.19	
Total:	2.105	

2^24	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)
	3.82	Neglible
	3.63	
Total:	3.725	

2^25	Parameter Generation (Execution Time)	Parameter Generation (Memory Utilization)
	6.33	Neglible
	6.13	
Total:	6.23	

CPU PROOF GENERATION

CPU Benchmarking — FIGURE 1

snark-challenge-prover-reference repository: https://github.com/TalDerei/snark-challenge-prover-reference

Execution Time = seconds
CPU Utilization = percent
Memory Utilization = GB

Intel(R) Xeon(R) Gold 5120 CPU @ 2.20GHz

OCPU count: 28 | Memory (GB): 192 GB | Network bandwidth (Gbps): 50 | Boot Disk: 128 GB

Size (2^15)

	CPU Program (Execution Time)	CPU Program (CPU Utilization)	CPU Program (Memory Utilization)
	5.36	100	0
	5.37	100	0
	5.37	100	0
Total:	5.366666667	100	0

	CPU MSM (Execution Time)	CPU FFT (Execution Time)
	4.81	0.54
	4.77	0.58
	4.76	0.57
Total:	4.78	0.5633333333

Size (2^16)

	CPU Program (Execution Time)	CPU Program (CPU Utilization)	CPU Program (Memory Utilization)
	9.53	100	0
	9.67	100	0
	9.65	100	0
Total:	9.616666667	100	0

	CPU MSM (Execution Time)	CPU FFT (Execution Time)
	8.54	0.95
	8.61	1.02
	8.6	1.02
Total:	8.583333333	0.9966666667

Size (2^17)

	CPU Program (Execution Time)	CPU Program (CPU Utilization)	CPU Program (Memory Utilization)
	18.3	100	0.48
	17.76	100	0.48
	17.85	100	0.48
Total:	17.97	100	0.48

	CPU MSM (Execution Time)	CPU FFT (Execution Time)
	15.79	2.42
	15.77	1.9
	15.76	2.1
Total:	15.77333333	2.14

Size (2^18)

	CPU Program (Execution Time)	CPU Program (CPU Utilization)	CPU Program (Memory Utilization)
	32.43	100	1.05
	32.45	100	1.05
	32.33	100	1.07
Total:	32.40333333	100	1.056666667

	CPU MSM (Execution Time)	CPU FFT (Execution Time)
	28.94	3.29
	28.64	3.62
	28.75	3.43
Total:	28.77666667	3.446666667

Size (2^19)

	CPU Program (Execution Time)	CPU Program (CPU Utilization)	CPU Program (Memory Utilization)
	60.96	100	2.13
	61.05	100	2.15
	61.03	100	2.13
Total:	61.01333333	100	2.136666667

	CPU MSM (Execution Time)	CPU FFT (Execution Time)
	53.83	6.67
	53.74	6.85
	53.8	6.84
Total:	53.79	6.786666667

Size (2^20)

	CPU Program (Execution Time)	CPU Program (CPU Utilization)	CPU Program (Memory Utilization)
	113.94	100	3.93
	113.4	100	3.93
	114.06	100	3.96
Total:	113.8	100	3.94

CPU Benchmarking — FIGURE 2

snark-challenge-prover-reference repository: https://github.com/TalDerei/snark-challenge-prover-reference

Execution Time = seconds
CPU Utilization = percent
Memory Utilization = GB

Intel(R) Xeon(R) Platinum 8358 CPU @ 2.60GHz

Core Count: 128 | Memory (GB): 1024 GB | Network bandwidth (Gbps): 50 | Boot Disk: 128 GB | Year: Q2 2021

Size (2^15)

	CPU Program (Execution Time)	CPU Program (CPU Utilization)	CPU Program (Memory Utilization)
	4.43	100	0
	4.51	100	0
	4.44	100	0
Total:	4.46	100	0

	CPU MSM (Execution Time)	CPU FFT (Execution Time)
	3.89	0.52
	3.96	0.53
	3.92	0.52
Total:	3.923333333	0.5233333333

Size (2^16)

	CPU Program (Execution Time)	CPU Program (CPU Utilization)	CPU Program (Memory Utilization)
	6.85	100	0
	6.86	100	0
	6.85	100	0
Total:	6.853333333	100	0

	CPU MSM (Execution Time)	CPU FFT (Execution Time)
	5.83	0.99
	5.78	1.05
	5.77	1.04
Total:	5.793333333	1.026666667

Size (2^17)

	CPU Program (Execution Time)	CPU Program (CPU Utilization)	CPU Program (Memory Utilization)
	12.17	100	0.52
	12.15	100	0.53
	12.2	100	0.52
Total:	12.17333333	100	0.5233333333

	CPU MSM (Execution Time)	CPU FFT (Execution Time)
	9.94	2.16
	9.94	2.14
	9.96	2.17
Total:	9.946666667	2.156666667

Size (2^18)

	CPU Program (Execution Time)	CPU Program (CPU Utilization)	CPU Program (Memory Utilization)
	21.36	100	0.92
	20.55	100	0.93
	20.72	100	0.93
Total:	20.87666667	100	0.9266666667

	CPU MSM (Execution Time)	CPU FFT (Execution Time)
	17.36	3.86
	16.67	3.72
	16.93	3.75
Total:	16.98666667	3.776666667

Size (2^19)

	CPU Program (Execution Time)	CPU Program (CPU Utilization)	CPU Program (Memory Utilization)
	34.62	100	1.74
	34.73	100	1.74
	34.53	100	1.74
Total:	34.62666667	100	1.74

	CPU MSM (Execution Time)	CPU FFT (Execution Time)
	27.01	7.38
	26.96	7.53
	26.99	7.45
Total:	26.98666667	7.453333333

Size (2^20)

	CPU Program (Execution Time)	CPU Program (CPU Utilization)	CPU Program (Memory Utilization)
	63.12	100	3.48
	63.72	100	3.38
	63.43	100	3.48
Total:	63.42333333	100	3.446666667

	CPU MSM (Execution Time)	CPU FFT (Execution Time)
	100.09	12.94
	98.97	13.5
	100.19	12.97
Total:	99.75	13.13666667

Size (2^21)

	CPU Program (Execution Time)	CPU Program (CPU Utilization)	CPU Program (Memory Utilization)
	211.62	100	7.85
	213.86	100	7.83
	212.34	100	7.87
Total:	212.6066667	100	7.85

	CPU MSM (Execution Time)	CPU FFT (Execution Time)
	185.84	23.94
	188.23	23.77
	186.3	24.17
Total:	186.79	23.96

Size (2^22)

	CPU Program (Execution Time)	CPU Program (CPU Utilization)	CPU Program (Memory Utilization)
	401.05	100	16.9
	401.58	100	16.86
	402.34	100	16.88
Total:	401.6566667	100	16.88

	CPU MSM (Execution Time)	CPU FFT (Execution Time)
	350.43	46.87
	349.68	48.13
	350.17	48.44
Total:	350.0933333	47.81333333

Size (2^23)

	CPU Program (Execution Time)	CPU Program (CPU Utilization)	CPU Program (Memory Utilization)
	773.43	100	30.85
	777.78	100	30.8
	774.68	100	30.82
Total:	775.2966667	100	30.82333333

	CPU MSM (Execution Time)	CPU FFT (Execution Time)
	667.2	98.66
	670.35	99.87
	672.33	98.5
Total:	669.96	99.01

Size (2^24)

	CPU Program (Execution Time)	CPU Program (CPU Utilization)	CPU Program (Memory Utilization)
	1490.77	100	61.54
	1492.15	100	61.67
	1493.25	100	61.86
Total:	1492.056667	100	61.69

	CPU MSM (Execution Time)	CPU FFT (Execution Time)
	1275.43	200.85
	1270.87	206.05
	1250.37	205.75
Total:	1265.556667	204.2166667

Size (2^25)

	CPU Program (Execution Time)	CPU Program (CPU Utilization)	CPU Program (Memory Utilization)
		Process killed due to insufficient memory (192 GB)	
Total:			

	CPU MSM (Execution Time)	CPU FFT (Execution Time)
Total:		

	CPU MSM (Execution Time)	CPU FFT (Execution Time)
	48.38	14.29
	49.3	13.96
	48.67	14.14
Total:	48.78333333	14.13

Size (2^21)

	CPU Program (Execution Time)	CPU Program (CPU Utilization)	CPU Program (Memory Utilization)
	113.34	100	6.94
	115.41	100	6.96
	112.93	100	7.07
Total:	113.8933333	100	6.99

	CPU MSM (Execution Time)	CPU FFT (Execution Time)
	88.25	24.2
	88.14	24.31
	89.74	24.74
Total:	88.71	24.41666667

Size (2^22)

	CPU Program (Execution Time)	CPU Program (CPU Utilization)	CPU Program (Memory Utilization)
	211.37	100	13.4
	211.42	100	13.31
	211.34	100	13.31
Total:	211.3766667	100	13.34

	CPU MSM (Execution Time)	CPU FFT (Execution Time)
	160.21	49.4
	158.76	50.84
	159.86	50.32
Total:	159.61	50.18666667

Size (2^23)

	CPU Program (Execution Time)	CPU Program (CPU Utilization)	CPU Program (Memory Utilization)
	361.82	100	26.73
	361.16	100	26.93
	361.73	100	26.73
Total:	361.57	100	26.79666667

	CPU MSM (Execution Time)	CPU FFT (Execution Time)
	258.73	99.61
	258.78	98.81
	258.75	99.52
Total:	258.7533333	99.31333333

Size (2^24)

	CPU Program (Execution Time)	CPU Program (CPU Utilization)	CPU Program (Memory Utilization)
	770.81	100	53.84
	771.35	100	53.81
	773.21	100	53.71
Total:	771.79	100	53.78666667

	CPU MSM (Execution Time)	CPU FFT (Execution Time)
	552.75	210.78
	553.21	211.72
	554.32	209.34
Total:	553.4266667	210.6133333

Size (2^25)

	CPU Program (Execution Time)	CPU Program (CPU Utilization)	CPU Program (Memory Utilization)
	1542.21	100	110.32
	1539.59	100	110.92
	1541.24	100	109.34
Total:	1541.013333	100	110.1933333

	CPU MSM (Execution Time)	CPU FFT (Execution Time)
	1110.12	425.32
	1113.43	425.42
	1114.24	422.35
Total:	1112.596667	424.3633333

GPU PROOF GENERATION

GPU Benchmarking — FIGURE 1

gpu-groth16-prover-3x: https://github.com/TalDerei/gpu-groth16-prover-3x

Execution Time = seconds
GPU Utilization = percent
Memory Utilization = GB

Note: MSM and FFTs run in parallel

Shape: BM.GPU2.2

GPUs	Architecture	GPU Interconnect	GPU Memory	GPU Cores	System Memory	Network
NVIDIA P100	Pascal	N/A	16 GB HBM2	3584	192 GB	2x 25 Gbps

Size (2^15)

GPU Program (Execution Time)	GPU Program (GPU Utilization)	GPU Program (VRAM Memory Utilization)	GPU Program (System Memory Utilization)
3.46	100	1.09	
3.47	100	1.09	
3.46	100	1.09	
Total: 3.463333333	100	1.09	0

GPU MSM (Execution Time)	GPU FFT (Execution Time)
3.44	0.64
3.42	0.67
3.43	0.67
Total: 3.43	0.66

Size (2^16)

GPU Program (Execution Time)	GPU Program (GPU Utilization)	GPU Program (VRAM Memory Utilization)	GPU Program (System Memory Utilization)
6.82	100	1.9	1.86
6.85	100	1.9	1.42
6.83	100	1.9	1.44
Total: 6.833333333	100	1.9	1.57333333

GPU MSM (Execution Time)	GPU FFT (Execution Time)
6.79	1.31
6.75	1.3
6.73	1.31
Total: 6.756666667	1.306666667

Size (2^17)

GPU Program (Execution Time)	GPU Program (GPU Utilization)	GPU Program (VRAM Memory Utilization)	GPU Program (System Memory Utilization)
13.94	100	3.51	3.57
14.31	100	3.51	3.55
14.22	100	3.51	3.55
Total: 14.15666667	100	3.51	3.55666667

GPU MSM (Execution Time)	GPU FFT (Execution Time)
13.88	1.97
14.25	1.95
13.92	1.93
Total: 14.01666667	1.95

Size (2^18)

GPU Program (Execution Time)	GPU Program (GPU Utilization)	GPU Program (VRAM Memory Utilization)	GPU Program (System Memory Utilization)
24.37	100	6.6	6.89
24.21	100	6.6	6.87
24.12	100	6.6	6.87
Total: 24.23333333	100	6.6	6.87666667

GPU MSM (Execution Time)	GPU FFT (Execution Time)
24.2	3.91
24.04	3.45
24.01	3.46
Total: 24.08333333	3.606666667

Size (2^19)

GPU Program (Execution Time)	GPU Program (GPU Utilization)	GPU Program (VRAM Memory Utilization)	GPU Program (System Memory Utilization)
46.7	100	12.9	13.81
47	100	12.9	13.77
46.85	100	12.9	13.75
Total: 46.85	100	12.9	13.77666667

GPU MSM (Execution Time)	GPU FFT (Execution Time)
46.33	6.94
46.63	7.14
46.44	7.05
Total: 46.46666667	7.043333333

Size (2^20)

GPU Program (Execution Time)	GPU Program (GPU Utilization)	GPU Program (VRAM Memory Utilization)	GPU Program (System Memory Utilization)
75.25	100	16	26.84
75.71	100	16	26.82
75.65	100	16	26.67
Total: 75.53666667	100	16	26.77666667

GPU MSM (Execution Time)	GPU FFT (Execution Time)
74.55	13.13
75.01	13.11
75.43	13.12
Total: 74.99666667	13.12

Size (2^21)

GPU Program (Execution Time)	GPU Program (GPU Utilization)	GPU Program (VRAM Memory Utilization)	GPU Program (System Memory Utilization)
176.26	100	16	54.66
176.69	100	16	53.47
176.75	100	16	53.78
Total: 176.5666667	100	16	53.97

GPU MSM (Execution Time)	GPU FFT (Execution Time)
174.71	26.2
175.16	25.54
175.32	25.73
Total: 175.0633333	25.82333333

Size (2^22)

GPU Program (Execution Time)	GPU Program (GPU Utilization)	GPU Program (VRAM Memory Utilization)	GPU Program (System Memory Utilization)
362.95	100	16	111.38
357.55	100	16	106.87
358.52	100	16	110.48
Total: 359.6733333	100	16	109.5766667

GPU MSM (Execution Time)	GPU FFT (Execution Time)
337.35	49.85
338.29	51.23
338.53	50.45
Total: 338.0566667	50.51

Size (2^23)

GPU Program (Execution Time)	GPU Program (GPU Utilization)	GPU Program (VRAM Memory Utilization)	GPU Program (System Memory Utilization)
Failed to read all curve poinst -- Aborted (core dumped)			
Not enough system memory to load in all the preprocessed curve points			
Total:			

GPU MSM (Execution Time)	GPU FFT (Execution Time)

Size (2^24)

GPU Program (Execution Time)	GPU Program (GPU Utilization)	GPU Program (VRAM Memory Utilization)	GPU Program (System Memory Utilization)
Failed to read all curve poinst -- Aborted (core dumped)			
Not enough system memory to load in all the preprocessed curve points			
Total:			

GPU Benchmarking — FIGURE 2

gpu-groth16-prover-3x: https://github.com/TalDerei/gpu-groth16-prover-3x

Execution Time = seconds
GPU Utilization = percent
Memory Utilization = GB

Note: MSM and FFTs run in parallel

Shape: BM.GPU.A10.4

GPUs	Architecture	GPU Interconne	GPU Memory	GPU Cores	System Memory	Network
Nvidia A10	Ampere	N/A	24 GB GDDR6	9216	1024 GB	2x 25 Gbps

Size (2^15)

GPU Program (Execution Time)	GPU Program (GPU Utilization)	GPU Program (VRAM Memory Utilization)	GPU Program (System Memory Utilization)
1.48	100	1.09	0
1.48	100	1.09	0
1.48	100	1.09	0
Total: 1.48	100	1.09	0

GPU MSM (Execution Time)	GPU FFT (Execution Time)
1.46	0.53
1.47	0.54
1.46	0.54
Total: 1.463333333	0.536666667

Size (2^16)

GPU Program (Execution Time)	GPU Program (GPU Utilization)	GPU Program (VRAM Memory Utilization)	GPU Program (System Memory Utilization)
2.09	100	1.9	1.02
2.15	100	1.9	1.02
2.13	100	1.9	1.02
Total: 2.123333333	100	1.9	1.02

GPU MSM (Execution Time)	GPU FFT (Execution Time)
2.07	1
2.12	0.98
2.1	0.99
Total: 2.096666667	0.99

Size (2^17)

GPU Program (Execution Time)	GPU Program (GPU Utilization)	GPU Program (VRAM Memory Utilization)	GPU Program (System Memory Utilization)
3.65	100	3.51	3.07
3.57	100	3.51	3.07
3.58	100	3.51	3.07
Total: 3.6	100	3.51	3.07

GPU MSM (Execution Time)	GPU FFT (Execution Time)
3.81	1.94
3.53	1.98
3.56	1.96
Total: 3.566666667	1.96

Size (2^18)

GPU Program (Execution Time)	GPU Program (GPU Utilization)	GPU Program (VRAM Memory Utilization)	GPU Program (System Memory Utilization)
6.61	100	6.6	6.96
6.43	100	6.6	6.76
6.45	100	6.6	6.86
Total: 6.496666667	100	6.6	6.86

GPU MSM (Execution Time)	GPU FFT (Execution Time)
6.52	3.65 100
6.33	3.9 100
6.43	3.74 100
Total: 6.426666667	3.763333333 100

Size (2^19)

GPU Program (Execution Time)	GPU Program (GPU Utilization)	GPU Program (VRAM Memory Utilization)	GPU Program (System Memory Utilization)
12.25	100	12.9	13.82
12.13	100	12.9	13.72
12.2	100	12.9	13.72
Total: 12.19333333	100	12.9	13.68666667

GPU MSM (Execution Time)	GPU FFT (Execution Time)
12.03	7.37
11.9	7.96
11.95	7.67
Total: 11.96	7.666666667

Size (2^20)

GPU Program (Execution Time)	GPU Program (GPU Utilization)	GPU Program (VRAM Memory Utilization)	GPU Program (System Memory Utilization)
23.26	100	24	21.91
23.32	100	24	22.01
23.29	100	24	22.01
Total: 23.29	100	24	21.97666667

GPU MSM (Execution Time)	GPU FFT (Execution Time)
22.81	14.58
22.86	14.82
22.89	14.75
Total: 22.85333333	14.71666667

Size (2^21)

GPU Program (Execution Time)	GPU Program (GPU Utilization)	GPU Program (VRAM Memory Utilization)	GPU Program (System Memory Utilization)
43.33	100	24	53.86
43.58	100	24	52.63
43.48	100	24	53.25
Total: 43.46333333	100	24	53.24666667

GPU MSM (Execution Time)	GPU FFT (Execution Time)
42.38	25.53
42.64	25.55
42.54	25.49
Total: 42.52	25.52333333

Size (2^22)

GPU Program (Execution Time)	GPU Program (GPU Utilization)	GPU Program (VRAM Memory Utilization)	GPU Program (System Memory Utilization)
86.94	100	24	107.83
87.32	100	24	107.72
86.99	100	24	107.83
Total: 87.08333333	100	24	107.7933333

GPU MSM (Execution Time)	GPU FFT (Execution Time)
85.06	51.91
85.4	50.45
85.32	50.96
Total: 85.26	51.10666667

Size (2^23)

GPU Program (Execution Time)	GPU Program (GPU Utilization)	GPU Program (VRAM Memory Utilization)	GPU Program (System Memory Utilization)
180.58	100	24	215.24
180.35	100	24	213.91
180.23	100	24	214.53
Total: 180.3866667	100	24	214.56

GPU MSM (Execution Time)	GPU FFT (Execution Time)
176.58	105.98
176.45	103.35
176.33	104.32
Total: 176.4533333	104.55

Size (2^24)

GPU Program (Execution Time)	GPU Program (GPU Utilization)	GPU Program (VRAM Memory Utilization)	GPU Program (System Memory Utilization)
378.29	100	24	429.47
377.38	100	24	429.26
378.21	100	24	429.16
Total: 377.96	100	24	429.2966667

	GPU MSM (Execution Time)	GPU FFT (Execution Time)
Total:		

Size (2^25)

	GPU Program (Execution Time)	GPU Program (GPU Utilization)	GPU Program (VRAM Memory Utilization)	GPU Program (System Memory Utilization)
		Failed to read all curve poinst -- Aborted (core dumped)		
Total:		Not enough system memory to load in all the preprocessed curve points		

	GPU MSM (Execution Time)	GPU FFT (Execution Time)
Total:		

	GPU MSM (Execution Time)	GPU FFT (Execution Time)
	358.29	210.05
	357.32	210.21
	359.32	211.24
Total:	358.31	210.5

Size (2^25)

	GPU Program (Execution Time)	GPU Program (GPU Utilization)	GPU Program (VRAM Memory Utilization)	GPU Program (System Memory Utilization)
	732.32	100	24	863.33
	733.42	100	24	863.64
	731.21	100	24	861.39
Total:	732.3166667	100	24	862.7866667

	GPU MSM (Execution Time)	GPU FFT (Execution Time)
	700.21	421.24
	700.11	421.82
	701.24	420.45
Total:	700.52	421.17

ZPrize (test-msm-gpu): https://github.com/TalDerei/test-msm-gpu — *Execution Time = seconds* — *VRAM Memory Utilization = GB* — FIGURE 4

Shape: A10

GPUs	Architecture	GPU Interconnect	GPU Memory	Only measuring the MSM execution time and memory utilization in this repository
Nvidia A10	Ampere	N/A	24 GB GDDR6	

Size (2^15)

	GPU MSM (Execution Time)	GPU Program (VRAM Memory Utilization)
	0.547	1.67
	0.494	1.67
	0.527	1.67
Total:	0.5226666667	1.67

Size (2^16)

	GPU MSM (Execution Time)	GPU Program (VRAM Memory Utilization)
	0.536	1.676
	0.512	1.676
	0.546	1.676
Total:	0.5313333333	1.676

Size (2^17)

	GPU MSM (Execution Time)	GPU Program (VRAM Memory Utilization)
	0.539	1.685
	0.533	1.685
	0.539	1.685
Total:	0.536	1.685

Size (2^18)

	GPU MSM (Execution Time)	GPU Program (VRAM Memory Utilization)
	0.555	1.707
	0.596	1.707
	0.602	1.707
Total:	0.5843333333	1.707

Size (2^19)

	GPU MSM (Execution Time)	GPU Program (VRAM Memory Utilization)
	0.648	1.75
	0.627	1.75
	0.597	1.75
Total:	0.624	1.75

Size (2^20)

	GPU MSM (Execution Time)	GPU Program (VRAM Memory Utilization)
	0.614	1.84
	0.633	1.84
	0.622	1.84
Total:	0.623	1.84

Size (2^21)

	GPU MSM (Execution Time)	GPU Program (VRAM Memory Utilization)
	0.812	2.01
	0.845	2.01
	0.805	2.01
Total:	0.8206666667	2.01

Size (2^22)

	GPU MSM (Execution Time)	GPU Program (VRAM Memory Utilization)
	0.95	2.35
	0.943	2.35
	0.976	2.35
Total:	0.9563333333	2.35

Size (2^23)

	GPU MSM (Execution Time)	GPU Program (VRAM Memory Utilization)
	1.08	3.04
	1.4	3.04
	1.3	3.04
Total:	1.26	3.04

Size (2^24)

	GPU MSM (Execution Time)	GPU Program (VRAM Memory Utilization)
	1.56	4.42
	1.51	4.42
	1.64	4.42
Total:	1.57	4.42

Size (2^25)

	GPU MSM (Execution Time)	GPU Program (VRAM Memory Utilization)
	2.67	7.17
	2.7	7.17
	2.68	7.17
Total:	2.683333333	7.17

ZPrize (test-msm-gpu): https://github.com/TalDerei/test-msm-gpu — *Execution Time = seconds* — *VRAM Memory Utilization = GB* — FIGURE 4

Shape: A40

GPUs	Architecture	GPU Interconnect	GPU Memory	Only measuring the MSM execution time and memory utilization in this repository
Nvidia A40	Ampere	N/A	48 GB GDDR6	

Size (2^15)

	GPU MSM (Execution Time)	GPU Program (VRAM Memory Utilization)
	0.24	2
	0.25	2
	0.23	2
Total:	0.24	2

Size (2^16)

	GPU MSM (Execution Time)	GPU Program (VRAM Memory Utilization)
	0.24	2.05
	0.24	2.05
	0.24	2.05
Total:	0.24	2.05

Size (2^17)

	GPU MSM (Execution Time)	GPU Program (VRAM Memory Utilization)
	0.25	2.08
	0.25	2.08
	0.25	2.08
Total:	0.25	2.08

Size (2^18)

	GPU MSM (Execution Time)	GPU Program (VRAM Memory Utilization)
	0.25	2.1
	0.25	2.1
	0.26	2.1
Total:	0.2533333333	2.1

Size (2^19)

	GPU MSM (Execution Time)	GPU Program (VRAM Memory Utilization)
	0.25	2.14
	0.23	2.14
	0.23	2.14
Total:	0.2366666667	2.14

Size (2^20)

	GPU MSM (Execution Time)	GPU Program (VRAM Memory Utilization)
	0.29	2.23
	0.25	2.23
	0.25	2.23
Total:	0.2633333333	2.23

Size (2^21)

	GPU MSM (Execution Time)	GPU Program (VRAM Memory Utilization)
	0.35	2.4
	0.31	2.4
	0.33	2.4
Total:	0.33	2.4

Size (2^22)

	GPU MSM (Execution Time)	GPU Program (VRAM Memory Utilization)
	0.45	2.75
	0.42	2.75
	0.45	2.75
Total:	0.44	2.75

Size (2^23)

	GPU MSM (Execution Time)	GPU Program (VRAM Memory Utilization)
	0.65	3.43
	0.59	3.43
	0.59	3.43
Total:	0.61	3.43

Size (2^24)

	GPU MSM (Execution Time)	GPU Program (VRAM Memory Utilization)
	0.96	4.81
	1.01	4.81
	0.97	4.81
Total:	0.98	4.81

Size (2^25)

	GPU MSM (Execution Time)	GPU Program (VRAM Memory Utilization)
	1.75	7.56
	1.74	7.56
	1.71	7.56
Total:	1.733333333	7.56

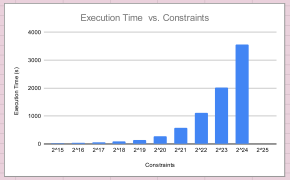
CHARTS

PARAMETER BENCHMARKING

FIGURE 1

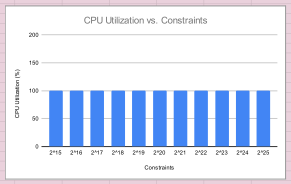
Parameter Generation (Execution Time)

Constraints	Execution Time
2^15	30.21
2^16	43.5
2^17	53.57
2^18	98.64
2^19	148.03
2^20	271.72
2^21	583.14
2^22	1114.58
2^23	2015.31
2^24	3566.13
2^25	N/A



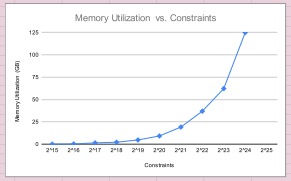
Parameter Generation (CPU Utilization)

Constraints	CPU Utilization
2^15	100
2^16	100
2^17	100
2^18	100
2^19	100
2^20	100
2^21	100
2^22	100
2^23	100
2^24	100
2^25	100



Parameter Generation (Memory Utilization)

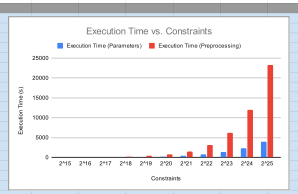
Constraints	Memory Utilization
2^15	0
2^16	0.19
2^17	1.43
2^18	2.16
2^19	4.69
2^20	9.18
2^21	19.11
2^22	36.91
2^23	62.21
2^24	124.91
2^25	N/A



FIGURES 2 + 3

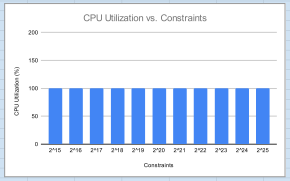
Parameter Generation (Execution Time)

Constraints	Execution Time (Parameters)	Execution Time (Preprocessing)
2^15	8.89	34.12
2^16	18.6	62.29
2^17	24.98	104.35
2^18	58.65	199.6
2^19	95.17	379.29
2^20	172	755
2^21	393.61	1501.91
2^22	759.71	3064.77
2^23	1360.04	6143.93
2^24	2233.07	11915.27
2^25	3904.49	23237.01



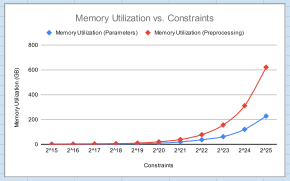
Parameter Generation (CPU Utilization)

Constraints	CPU Utilization
2^15	100
2^16	100
2^17	100
2^18	100
2^19	100
2^20	100
2^21	100
2^22	100
2^23	100
2^24	100
2^25	100



Parameter Generation (Memory Utilization)

Constraints	Memory Utilization (Parameters)	Memory Utilization (Preprocessing)
2^15	0	0
2^16	0.512	1.02
2^17	1.02	2.46
2^18	2.46	4.87
2^19	4.76	9.83
2^20	8.855	20.12
2^21	19.2	38.66
2^22	36.915	77.98
2^23	61.555	156.09
2^24	120.535	311.02
2^25	227.479	620.83



Parameter Generation (File Constraints)

Constraints	Input File	Parameter File	Preprocessing File
2^15	0.13	0.37	0.745
2^16	0.25	0.73	1.5
2^17	0.49	0.15	3
2^18	0.97	0.31	5.9
2^19	0.193	0.58	12
2^20	0.39	1.2	24
2^21	0.77	2.3	47
2^22	1.6	4.6	94
2^23	3.1	9.1	187
2^24	6.1	19	373
2^25	12.2	40	751

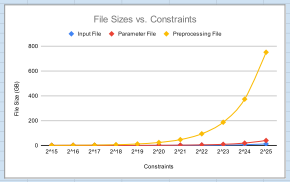
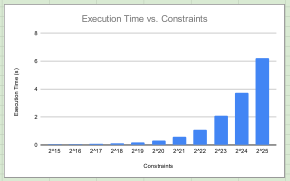


FIGURE 4

Parameter Generation (Execution Time)

Constraints	Execution Time
2^15	0.05
2^16	0.06
2^17	0.08
2^18	0.11
2^19	0.17
2^20	0.31
2^21	0.57
2^22	1.09
2^23	2.105
2^24	3.73
2^25	6.23

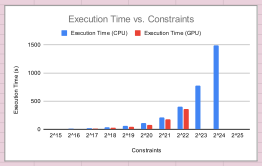


CPU / GPU BENCHMARKING

FIGURE 1 (CPU and GPU) on P100

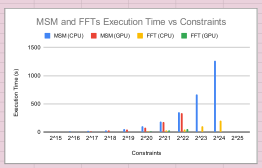
CPU and GPU Program (Execution Time)

Constraints	Execution Time (CPU)	Execution Time (GPU)
2^15	5.37	3.46
2^16	9.62	6.83
2^17	17.97	14.16
2^18	32.4	24.23
2^19	61.01	46.85
2^20	113.8	75.54
2^21	212.61	176.56
2^22	401.66	359.67
2^23	775.31	N/A
2^24	1492.06	N/A
2^25	N/A	N/A



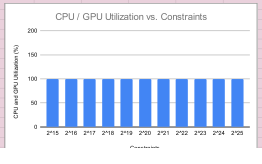
CPU and GPU Program (MSM and FFT)

Constraints	MSM (CPU)	MSM (GPU)	FFT (CPU)	FFT (GPU)
2^15	4.78	3.43	0.56	0.66
2^16	8.58	6.76	1.01	1.31
2^17	15.77	14.02	2.14	1.95
2^18	28.78	24.08	3.45	3.61
2^19	53.79	46.47	6.79	7.04
2^20	99.75	75	13.14	13.12
2^21	186.79	175.06	23.96	25.82
2^22	350.09	338.06	47.81	50.51
2^23	669.96	N/A	99.01	N/A
2^24	1265.56	N/A	204.22	N/A
2^25	N/A	N/A	N/A	N/A



CPU and GPU Program (CPU / GPU Utilization)

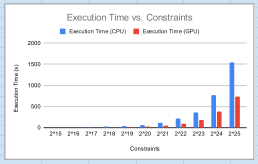
Constraints	CPU and GPU Utilization
2^15	100
2^16	100
2^17	100
2^18	100
2^19	100
2^20	100
2^21	100
2^22	100
2^23	100
2^24	100
2^25	100



FIGURES 2 (CPU and GPU) on A10

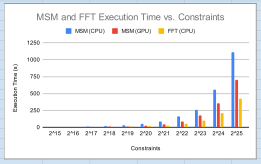
CPU and GPU Program (Execution Time)

Constraints	Execution Time (CPU)	Execution Time (GPU)
2^15	4.46	1.48
2^16	6.85	2.12
2^17	12.17	3.6
2^18	20.88	6.51
2^19	34.63	12.19
2^20	63.42	23.29
2^21	113.89	43.46
2^22	211.38	87.08
2^23	361.57	180.39
2^24	771.79	377.96
2^25	1541.01	732.32



CPU and GPU Program (MSM and FFT)

Constraints	MSM (CPU)	MSM (GPU)	FFT (CPU)
2^15	3.92	1.46	0.52
2^16	5.79	2.11	1.03
2^17	9.95	3.57	2.16
2^18	16.99	6.43	3.78
2^19	26.99	11.96	7.45
2^20	48.78	22.85	14.13
2^21	88.71	42.52	24.42
2^22	159.61	85.26	50.19
2^23	258.75	176.45	99.31
2^24	553.43	358.31	210.61
2^25	1112.61	700.52	424.36



CPU and GPU Program (CPU / GPU Utilization)

Constraints	CPU and GPU Utilization
2^15	100
2^16	100
2^17	100
2^18	100
2^19	100
2^20	100
2^21	100
2^22	100
2^23	100
2^24	100
2^25	100

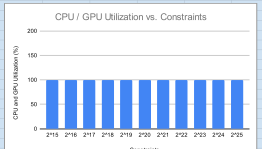
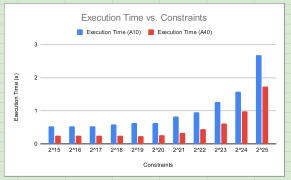


FIGURE 4 GPU on A40

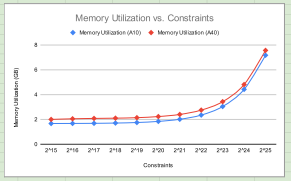
GPU Program (Execution Time)

Constraints	Execution Time (A10)	Execution Time (A40)
2^15	0.523	0.24
2^16	0.531	0.24
2^17	0.536	0.25
2^18	0.584	0.253
2^19	0.624	0.237
2^20	0.623	0.283
2^21	0.821	0.33
2^22	0.956	0.44
2^23	1.26	0.61
2^24	1.57	0.98
2^25	2.683	1.733



GPU Program (GPU Memory Utilization)

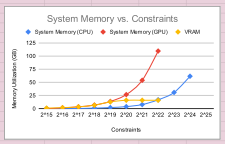
Constraints	Memory Utilization (A10)	Memory Utilization (A40)
2^15	1.67	2
2^16	1.676	2.05
2^17	1.685	2.08
2^18	1.707	2.1
2^19	1.75	2.14
2^20	1.84	2.23
2^21	2.01	2.4
2^22	2.35	2.75
2^23	3.04	3.43
2^24	4.42	4.81
2^25	7.17	7.56



Constraints

CPU and GPU Program (System Memory Utilization)

Constraints	System Memory (CPU)	System Memory (GPU)	VRAM
2^15	0	0	1.09
2^16	0	1.57	1.9
2^17	0.48	3.56	3.51
2^18	1.06	6.88	6.6
2^19	2.14	13.78	12.9
2^20	3.94	26.78	16
2^21	7.85	53.97	16
2^22	16.88	109.58	16
2^23	30.82	N/A	N/A
2^24	61.69	N/A	N/A
2^25	N/A	N/A	N/A



Constraints

CPU and GPU Program (System Memory Utilization)

Constraints	System Memory (CPU)	System Memory (GPU)	VRAM
2^15	0	0	1.09
2^16	0	1.02	1.9
2^17	0.52	3.07	3.51
2^18	0.93	6.86	6.6
2^19	1.74	13.69	12.9
2^20	3.45	21.98	24
2^21	6.99	53.25	24
2^22	13.34	107.79	24
2^23	26.8	214.56	24
2^24	53.79	429.3	24
2^25	110.19	862.79	24