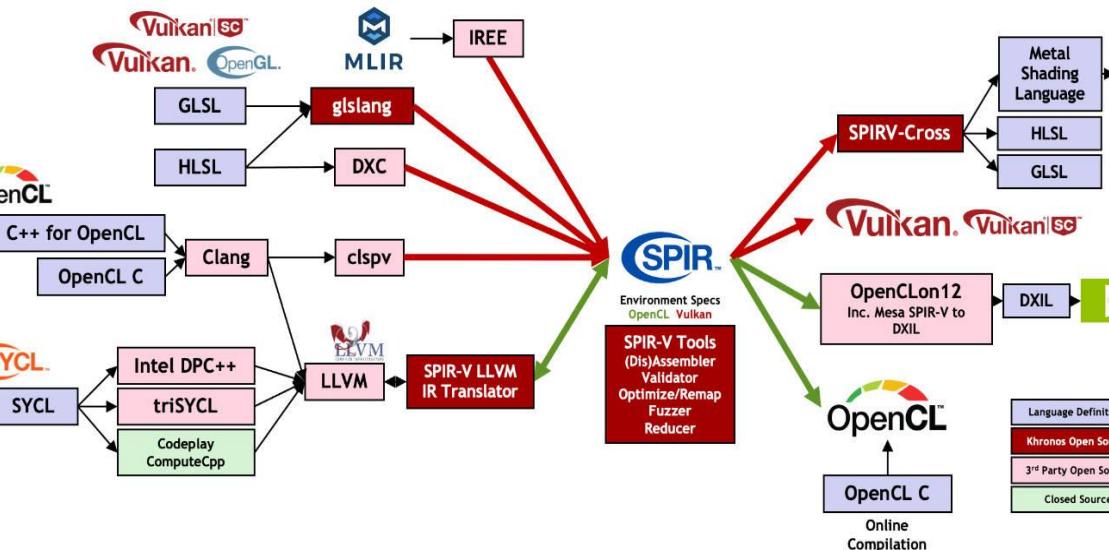
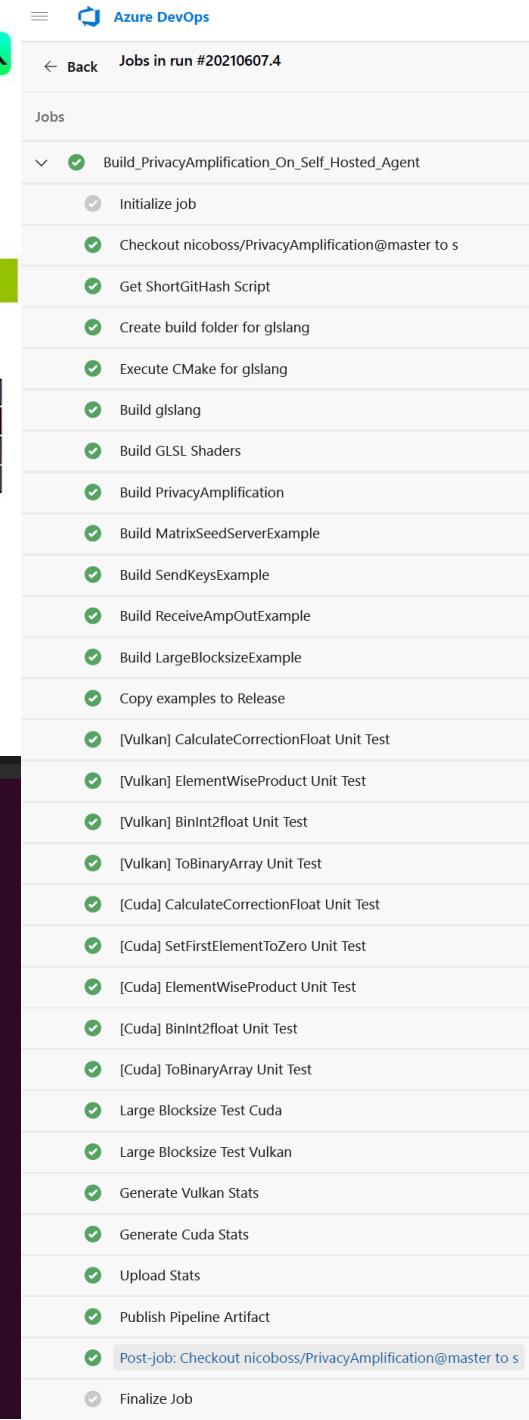


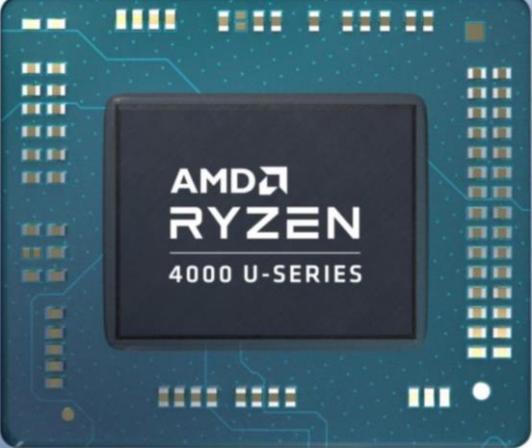
Function	Cuda	Vulkan	Differnece	Differnece %
			Vulkan - Cuda	((Vu/Cu)*100)-100
wait_for_input_buffer [ms]	0.006	0.006	0	0
cleaned_memory [ms]	0.003	0	-0.003	-100 %
set_count_to_zero [ms]	0.007	0.172	0.165	2'357 %
binIntffloat_seed [ms]	2.782	3.043	0.261	9 %
binIntffloat_key [ms]	1.762	1.991	0.229	13 %
calculateCorrectionFloat [ms]	0.068	0.226	0.158	232 %
fft_key [ms]	7.225	6.283	-0.942	-13 %
fft_seed [ms]	7.425	6.638	-0.787	-11 %
setFirstElementToZero [ms]	0.094	0	-0.094	-100 %
elementWiseProduct [ms]	2.397	2.467	0.07	3 %
ifft [ms]	7.352	6.65	-0.702	-10 %
wait_for_output_buffer [ms]	0.005	0.003	-0.002	-40 %
toBinaryArray [ms]	1.725	1.612	-0.113	-7 %
Total [ms]	30.868	29.094	-1.774	-6 %
Speed [MBit/s]	4348.055	4613.213	265.158	6 %



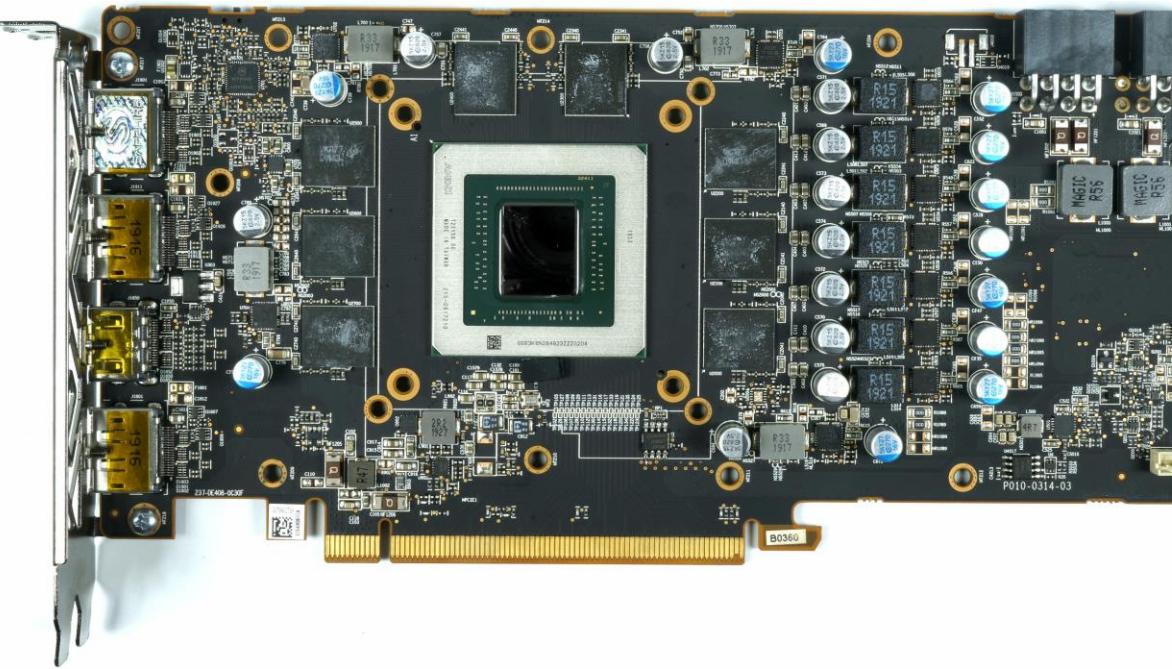
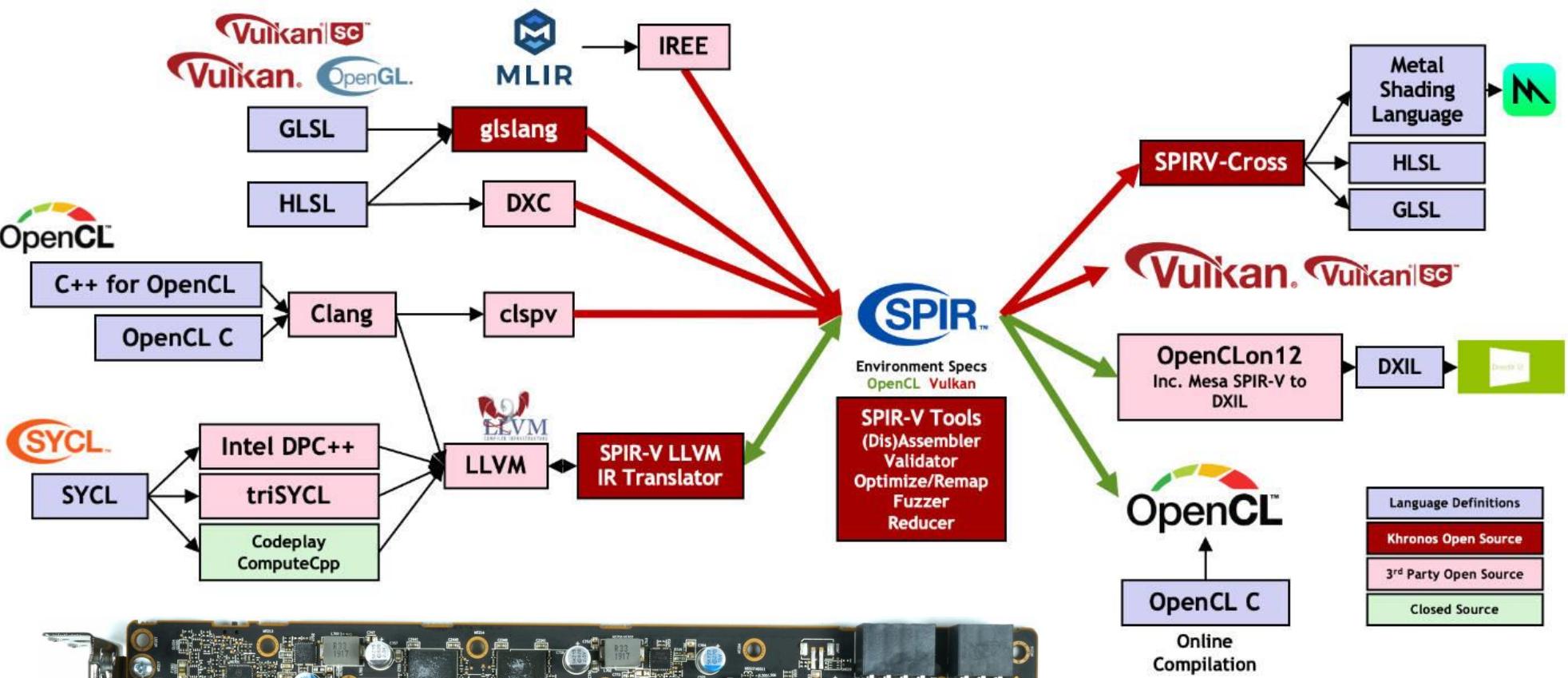
PRIVACY AMPLIFICATION



C:\Users\nico\Documents\GitHub\privacyamplification\



```
Blocktime: 131.475 ms => 255.215 Mbit/s
Blocktime: 133.707 ms => 250.955 Mbit/s
Blocktime: 134.251 ms => 249.938 Mbit/s
Blocktime: 132.842 ms => 252.589 Mbit/s
Blocktime: 134.543 ms => 249.396 Mbit/s
Blocktime: 132.806 ms => 252.658 Mbit/s
Blocktime: 133.797 ms => 250.786 Mbit/s
Blocktime: 135.952 ms => 246.811 Mbit/s
Blocktime: 133.754 ms => 250.867 Mbit/s
Blocktime: 133.56 ms => 251.231 Mbit/s
Blocktime: 134.03 ms => 250.35 Mbit/s
Blocktime: 131.628 ms => 254.919 Mbit/s
Blocktime: 133.627 ms => 251.105 Mbit/s
Blocktime: 132.521 ms => 253.201 Mbit/s
Blocktime: 133.6 ms => 251.156 Mbit/s
Blocktime: 132.835 ms => 252.602 Mbit/s
Blocktime: 133.141 ms => 252.022 Mbit/s
Blocktime: 131.26 ms => 255.633 Mbit/s
Blocktime: 135.7 ms => 247.269 Mbit/s
Blocktime: 134.939 ms => 248.664 Mbit/s
wait_for_input_buffer 0.000 ms
cleaned_memory 0.000 ms
set_count_to_zero 0.035 ms
binIntffloat_seed 4.473 ms
binIntffloat_key 2.502 ms
calculateCorrectionFloat 0.234 ms
fft_key 34.564 ms
fft_seed 38.718 ms
setFirstElementToZero 0.000 ms
elementWiseProduct 12.437 ms
ifft 35.738 ms
wait_for_output_buffer 0.000 ms
toBinaryArray 1.866 ms
Total 130.567 ms
Speed 256.991 MBit/s
```



```
Blocktime: 162.969 ms => 823.578 Mbit/s
Blocktime: 163.428 ms => 821.265 Mbit/s
Blocktime: 163.383 ms => 821.491 Mbit/s
Blocktime: 163.038 ms => 823.23 Mbit/s
Blocktime: 163.839 ms => 819.205 Mbit/s
Blocktime: 163.738 ms => 819.71 Mbit/s
wait_for_input_buffer 0.006 ms
cleaned_memory 0.000 ms
set_count_to_zero 0.161 ms
binIntffloat_seed 5.027 ms
binIntffloat_key 3.328 ms
calculateCorrectionFloat 0.153 ms
fft_key 47.156 ms
fft_seed 50.632 ms
setFirstElementToZero 0.000 ms
elementWiseProduct 4.259 ms
ifft 50.070 ms
wait_for_output_buffer 0.009 ms
toBinaryArray 2.013 ms
Total 162.818 ms
Speed 824.341 Mbit/s
```

```
Windows PowerShell
0x14: 00010100
0x9F: 10011111
0xDF: 11011111
0x49: 01001001
VERIFIED!
zmq_send: 6291456
16777220
Blocktime: 165.64 ms => 810.298 Mbit/
0x93: 10010011
0x45: 01000101
0x45: 010000101
0x7D: 01111101
0x14: 00010100
0x9F: 10011111
0xDF: 11011111
0x49: 01001001
VERIFIED!
zmq_send: 6291456
16777220
Blocktime: 165.898 ms => 809.038 Mbit
0x93: 10010011
0x45: 01000101
0x45: 010000101
0x7D: 01111101
0x14: 00010100
0x9F: 10011111
0xDF: 11011111
0x49: 01001001
VERIFIED!
```

File	Time	Event Type	Source
2021-06-08	21:21:19	Sent	Key
2021-06-08	21:21:19	Sent	Key
2021-06-08	21:21:19	Sent	Key
2021-06-08	21:21:19	Sent	Key
2021-06-08	21:21:20	Sent	Key
2021-06-08	21:21:20	Sent	Key
2021-06-08	21:21:20	Sent	Key
2021-06-08	21:21:20	Sent	Key
2021-06-08	21:21:20	Sent	Key
2021-06-08	21:21:20	Sent	Key
2021-06-08	21:21:20	Sent	Key
2021-06-08	21:21:20	Sent	Key
2021-06-08	21:21:21	Sent	Key
2021-06-08	21:21:21	Sent	Key
2021-06-08	21:21:21	Sent	Key
2021-06-08	21:21:21	Sent	Key
2021-06-08	21:21:21	Sent	Key
2021-06-08	21:21:21	Sent	Key
2021-06-08	21:21:21	Sent	Key
2021-06-08	21:21:22	Sent	Key
2021-06-08	21:21:22	Sent	Key
2021-06-08	21:21:22	Sent	Key
2021-06-08	21:21:22	Sent	Key
2021-06-08	21:21:22	Sent	Key
2021-06-08	21:21:23	Sent	Key
2021-06-08	21:21:23	Sent	Key
2021-06-08	21:21:23	Sent	Key
2021-06-08	21:21:23	Sent	Key
2021-06-08	21:21:23	Sent	Key
2021-06-08	21:21:23	Sent	Key
2021-06-08	21:21:24	Sent	Key

TechPowerUp GPU-Z 2.40.0				
Graphics Card		Sensors	Advanced	Validation
Name				AMD Radeon RX 5700 XT
GPU	Navi 10	Revision	00	Loc
Technology	7 nm	Die Size	251 mm ²	AM Radeon
Release Date	Jul 7, 2019	Transistors	10300M	Graph
BIOS Version	Unknown			
Subvendor	AMD/ATI	Device ID	1002 731F - 1002	
ROPs/TMUs	64 / 160	Bus Interface	PCI	
Shaders	2560 Unified	DirectX Support	12 (1)	
Pixel Fllrate	121.9 GPixel/s	Texture Fllrate	304.8 GTexel/s	
Memory Type	GDDR6 (Samsung)	Bus Width	256 bit	
Memory Size	0 MB	Bandwidth	448.0 GB/s	
Driver Version	27.20.21002.112 (Adrenalin 21.4.1) DCH / Win10			
Driver Date	Apr 13, 2021	Digital Signature	WHQL	
GPU Clock	1755 MHz	Memory	1750 MHz	Boost 1900 MHz
Default Clock	1755 MHz	Memory	1750 MHz	Boost 1900 MHz
AMD CrossFire	Disabled	Resizable BAR	Disabled	
Computing	<input checked="" type="checkbox"/> OpenCL	<input type="checkbox"/> CUDA	<input checked="" type="checkbox"/> DirectCompute	<input checked="" type="checkbox"/> Dispatch
Technologies	<input checked="" type="checkbox"/> Vulkan	<input type="checkbox"/> Ray Tracing	<input type="checkbox"/> PhysX	<input checked="" type="checkbox"/> OpenGL

AMD Radeon RX 5700 XT	
Graphics Card Sensors Advanced Validation	
GPU Clock	2012.0 MHz
Memory Clock	1742.0 MHz
UVD Clock	0.0 MHz
UVD Clock	0.0 MHz
GPU Temperature	40.0 °C
GPU Temperature (Hot Spot)	45.0 °C
Memory Temperature	56.0 °C
GPU VRM Temperature	46.0 °C
Mem1 VRM Temperature	42.0 °C
Mem2 VRM Temperature	44.0 °C
Fan Speed (%)	0 %
Fan Speed (RPM)	0 RPM
GPU Load	99 %
Memory Controller Load	12 %
Memory Used (Dedicated)	3281 MB
Log to file	<input type="checkbox"/>

File	Path	Content
		2021-06-08 21:21:19 Sent Seed to Client Alice
		2021-06-08 21:21:19 Sent Seed to Client Alice
		2021-06-08 21:21:19 Sent Seed to Client Alice
		2021-06-08 21:21:19 Sent Seed to Client Alice
		2021-06-08 21:21:20 Sent Seed to Client Alice
		2021-06-08 21:21:20 Sent Seed to Client Alice
		2021-06-08 21:21:20 Sent Seed to Client Alice
		2021-06-08 21:21:20 Sent Seed to Client Alice
		2021-06-08 21:21:20 Sent Seed to Client Alice
		2021-06-08 21:21:20 Sent Seed to Client Alice
		2021-06-08 21:21:20 Sent Seed to Client Alice
		2021-06-08 21:21:21 Sent Seed to Client Alice
		2021-06-08 21:21:21 Sent Seed to Client Alice
		2021-06-08 21:21:21 Sent Seed to Client Alice
		2021-06-08 21:21:21 Sent Seed to Client Alice
		2021-06-08 21:21:21 Sent Seed to Client Alice
		2021-06-08 21:21:21 Sent Seed to Client Alice
		2021-06-08 21:21:22 Sent Seed to Client Alice
		2021-06-08 21:21:22 Sent Seed to Client Alice
		2021-06-08 21:21:22 Sent Seed to Client Alice
		2021-06-08 21:21:22 Sent Seed to Client Alice
		2021-06-08 21:21:22 Sent Seed to Client Alice
		2021-06-08 21:21:22 Sent Seed to Client Alice
		2021-06-08 21:21:23 Sent Seed to Client Alice
		2021-06-08 21:21:23 Sent Seed to Client Alice
		2021-06-08 21:21:23 Sent Seed to Client Alice
		2021-06-08 21:21:23 Sent Seed to Client Alice
		2021-06-08 21:21:23 Sent Seed to Client Alice
		2021-06-08 21:21:24 Sent Seed to Client Alice

se	Windows PowerShell
2021-06-08 21:21:19	Key Block received
2021-06-08 21:21:20	Key Block received
2021-06-08 21:21:21	Key Block received
2021-06-08 21:21:22	Key Block received
2021-06-08 21:21:23	Key Block received
2021-06-08 21:21:24	Key Block received
2021-06-08 21:21:24	Key Block received

The screenshot shows the Windows Task Manager with the GPU tab selected. The main area displays four performance charts for different GPU workloads:

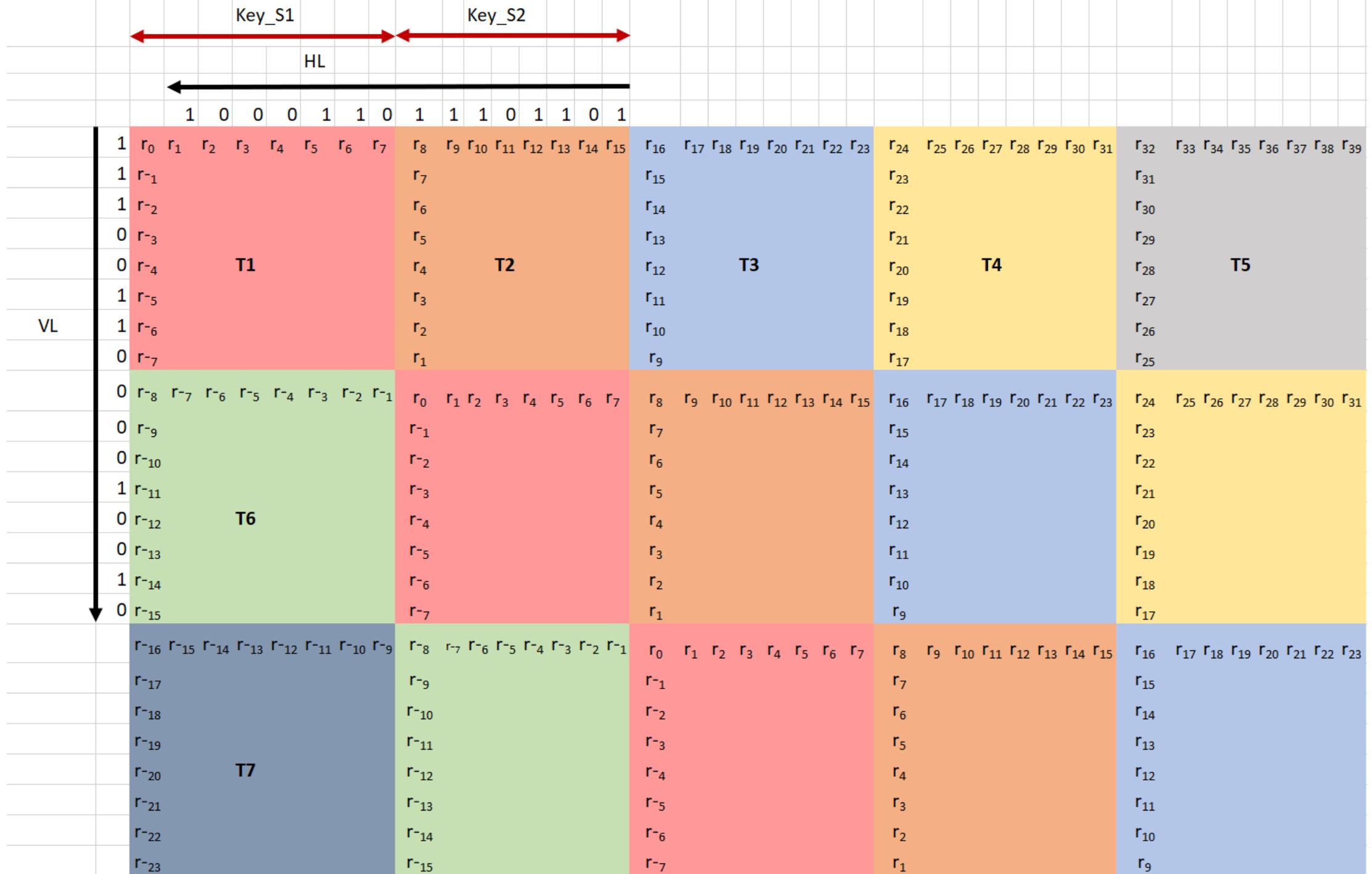
- 3D:** Shows a chart with a single data series at 99% utilization.
- Copy:** Shows a chart with a single data series at 0% utilization.
- High Priority 3D:** Shows a chart with a single data series at 0% utilization.
- High Priority Compute:** Shows a chart with a single data series at 0% utilization.

Below the charts, detailed memory usage statistics are provided:

Type	Usage
Dedicated GPU memory usage	8.0 GB
Shared GPU memory usage	12.0 GB

At the bottom, key GPU metrics are listed:

Metric	Value
Utilization	99%
Dedicated GPU memory	3.2/8.0 GB
GPU Memory	5.8/20.0 GB
Shared GPU memory	2.6/12.0 GB
GPU Temperature	46 °C



run.sh should run the Cuda version as it's the only one automatically... ...	Verified	bf1e8ad	🔗
Made speedtest Linux compatible nicoboss committed yesterday ✓	Verified	e2347cd	🔗
Marked executable files as executable using Linux file permissions nicoboss committed yesterday ✓	Verified	46e229d	🔗
PrivacyAmplification Vulkan works on Linux nicoboss committed yesterday ✓	Verified	daf299a	🔗

Commits on Jun 6, 2021

Fixed all LargeBlockSizeExample warnings nicoboss committed 2 days ago ✓	Verified	07335a0	🔗
Added LargeBlockSizeExample Linux Makefile nicoboss committed 2 days ago ✓	Verified	dcb9b6a	🔗
Fixed some warnings and improved readability by eliminating the PLAN... ... nicoboss committed 2 days ago ✓	Verified	ed1c328	🔗
Speedtest unrelated std::output must have a #-Prefix so it doesn't mess... ... nicoboss committed 2 days ago ✓	Verified	2elea3d	🔗
CUDA: Check driver compatibility and print device information nicoboss committed 2 days ago ✘	Verified	19e4789	🔗
Updated VkFFT due to better error and issue handling and most compile... ... nicoboss committed 2 days ago ✓	Verified	636197b	🔗
downloadAssets.cmd: Fixed the AzureCLI and azure-devops installation nicoboss committed 2 days ago ✓	Verified	ba9e1ca	🔗

Commits on Jun 5, 2021

Let's enable servers and not enable verify_ampout as otherwise "Large... ...	Verified	ae29fe3	🔗
Fixed Vulkan di1 and di2 required memory calculation issue caused by nicoboss committed 3 days ago ✘	Verified	e8a5854	🔗
Merge branch 'vkFFT_2_pow_14_vulkan_testing' nicoboss committed 3 days ago	Verified	3dc3c8	🔗
Write something before and after the two long pipeline tests so the u... ... nicoboss committed 3 days ago ✘	Verified	410eb30	🔗
Reverted pipeline tests back to 2^27 nicoboss committed 3 days ago	Verified	bd685da	🔗
azure-pipelines.yml: Run LargeBlockSizeTest for both Cuda and Vuda nicoboss committed 3 days ago ✓	Verified	c688bef	🔗
Let's not enable verify_ampout as otherwise "Large Blocksize Test" fails nicoboss committed 3 days ago ✓	Verified	13ea5a8	🔗
Fixed Cuda not working properly with seed caching nicoboss committed 3 days ago ✘	Verified	1e2faa6	🔗
Fixed reuse_seed_amount = -1 for static seed nicoboss committed 3 days ago ✘	Verified	fcd3a42	🔗
Implemented seed caching nicoboss committed 3 days ago ✘	Verified	996fb54	🔗
Fixed calculation difference between LargeBlockSizeExample and the no... ... nicoboss committed 3 days ago ✘	Verified	a466e4a	🔗
Added missing bracket nicoboss committed 4 days ago ✓	Verified	733fd2c	🔗

Azure DevOps			
← Back Jobs in run #20210607.4			
Jobs			
Build_PrivacyAmplification_On_Self_Hosted_Agent			
Initialize job			
Checkout nicoboss/PrivacyAmplification@master to s			
Get ShortGitHash Script			
Create build folder for glslang			
Execute CMake for glslang			
Build glslang			
Build GLSL Shaders			
Build PrivacyAmplification			
Build MatrixSeedServerExample			
Build SendKeysExample			
Build ReceiveAmpOutExample			
Build LargeBlockSizeExample			
Copy examples to Release			
[Vulkan] CalculateCorrectionFloat Unit Test			
[Vulkan] ElementWiseProduct Unit Test			
[Vulkan] BinInt2float Unit Test			
[Vulkan] ToBinaryArray Unit Test			
[Cuda] CalculateCorrectionFloat Unit Test			
[Cuda] SetFirstElementToZero Unit Test			
[Cuda] ElementWiseProduct Unit Test			
[Cuda] BinInt2float Unit Test			
[Cuda] ToBinaryArray Unit Test			
Large Blocksize Test Cuda			
Large Blocksize Test Vulkan			
Generate Vulkan Stats			
Generate Cuda Stats			
Upload Stats			
Publish Pipeline Artifact			
Post-job: Checkout nicoboss/PrivacyAmplification@master to s			
Finalize Job			

	File	Blocktime	Size
	0xDF: 11011111		
	0x49: 01001001		
	VERIFIED!		
	zmq_send: 6291456		
	16777220		
	Blocktime: 55.745 ms => 2407.71 Mbit/s		
	0x93: 10010011		
	0x45: 01000101		
	0x45: 01000101		
	0x7D: 01111101		
	0x14: 00010100		
	0x9F: 10011111		
	0xDF: 11011111		
	0x49: 01001001		
	VERIFIED!		
	zmq_send: 6291456		
	16777220		
	Blocktime: 57.101 ms => 2350.53 Mbit/s		
	0x93: 10010011		
	0x45: 01000101		
	0x45: 01000101		
	0x7D: 01111101		
	0x14: 00010100		
	0x9F: 10011111		
	0xDF: 11011111		
	0x49: 01001001		

2021-05-30 19:35:51 Sent Key
2021-05-30 19:35:52 Sent Key
2021-05-30 19:35:53 Sent Key
2021-05-30 19:35:53 Sent Key

root@Castleuntu: ~/privacyamplification

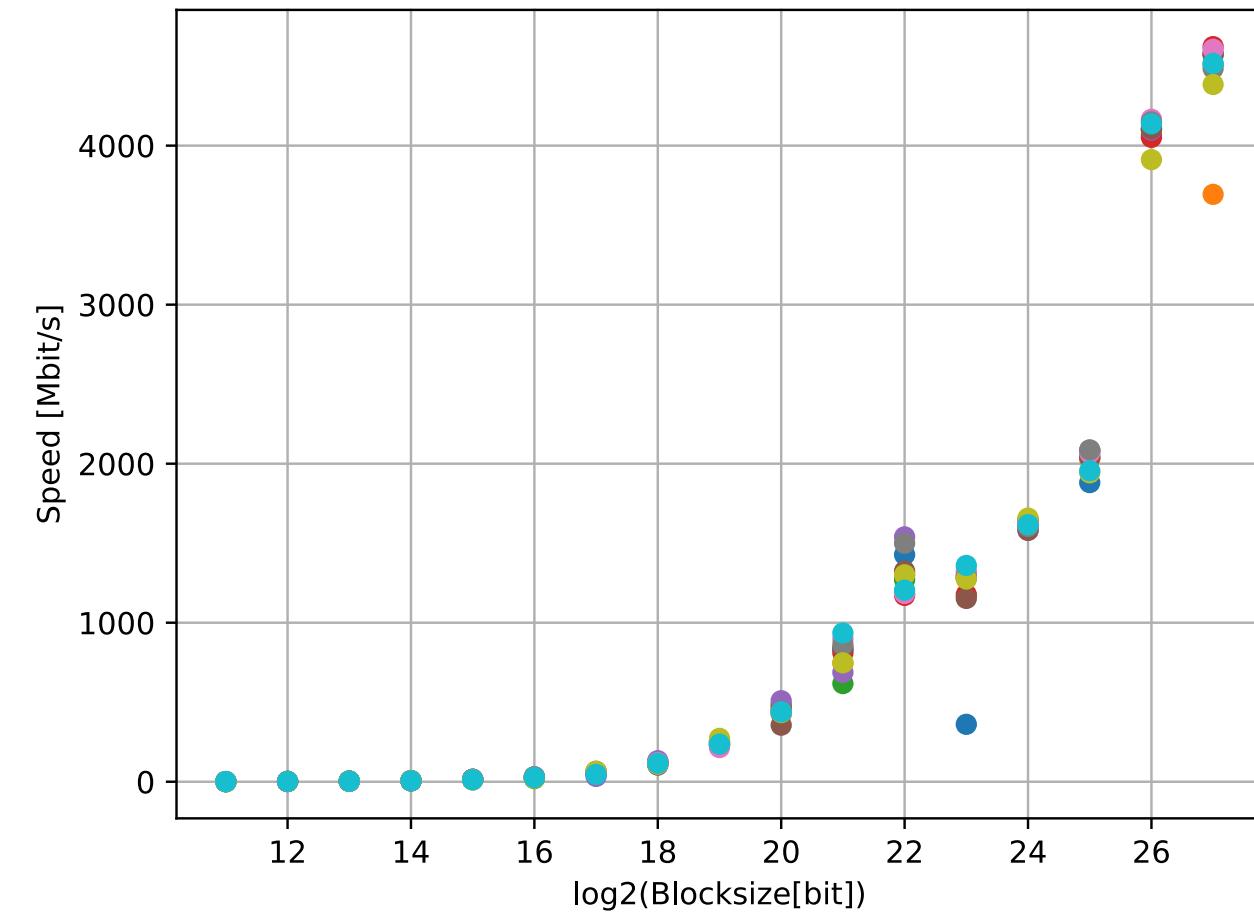
2021-05-30 19:35:51 Key Block received
2021-05-30 19:35:52 Key Block received
2021-05-30 19:35:53 Key Block received
2021-05-30 19:35:53 Key Block received

```
1500 -     cudaMallocHost((void**)&toeplitz_seed, input_cache_block_size * sizeof(uint32_t) * input_blocks_to_cache);
1501 -     cudaMallocHost((void**)&key_start, input_cache_block_size * sizeof(uint32_t) * input_blocks_to_cache);
1502 -     cudaMallocHost((void**)&key_rest, input_cache_block_size * sizeof(uint32_t) * input_blocks_to_cache + 31 * sizeof(uint32_t));
1503 -     cudaMallocHost((void**)&output, output_cache_block_size * output_blocks_to_cache);
1491 +     cudaMallocHost((void**)&toeplitz_seed, sizeof(uint32_t*) * input_blocks_to_cache);
1492 +     for (int i = 0; i < input_blocks_to_cache; ++i) {
1493 +         cudaMallocHost((void**)&toeplitz_seed[i], sizeof(uint32_t) * input_cache_block_size);
1494 +     }
1495 +     cudaMallocHost((void**)&key_start, sizeof(uint32_t*) * input_blocks_to_cache);
1496 +     for (int i = 0; i < input_blocks_to_cache; ++i) {
1497 +         cudaMallocHost((void**)&key_start[i], sizeof(uint32_t) * input_cache_block_size);
1498 +     }
1499 +     cudaMallocHost((void**)&key_rest, sizeof(uint32_t*) * input_blocks_to_cache);
1500 +     for (int i = 0; i < input_blocks_to_cache; ++i) {
1501 +         cudaMallocHost((void**)&key_rest[i], sizeof(uint32_t) * input_cache_block_size + 31 * sizeof(uint32_t));
1502 +     }
1503 +     cudaMallocHost((void**)&output, sizeof(uint8_t*) * output_blocks_to_cache);
1504 +     for (int i = 0; i < output_blocks_to_cache; ++i) {
1505 +         cudaMallocHost((void**)&output[i], sizeof(uint8_t) * output_cache_block_size);
1506 +     }
```

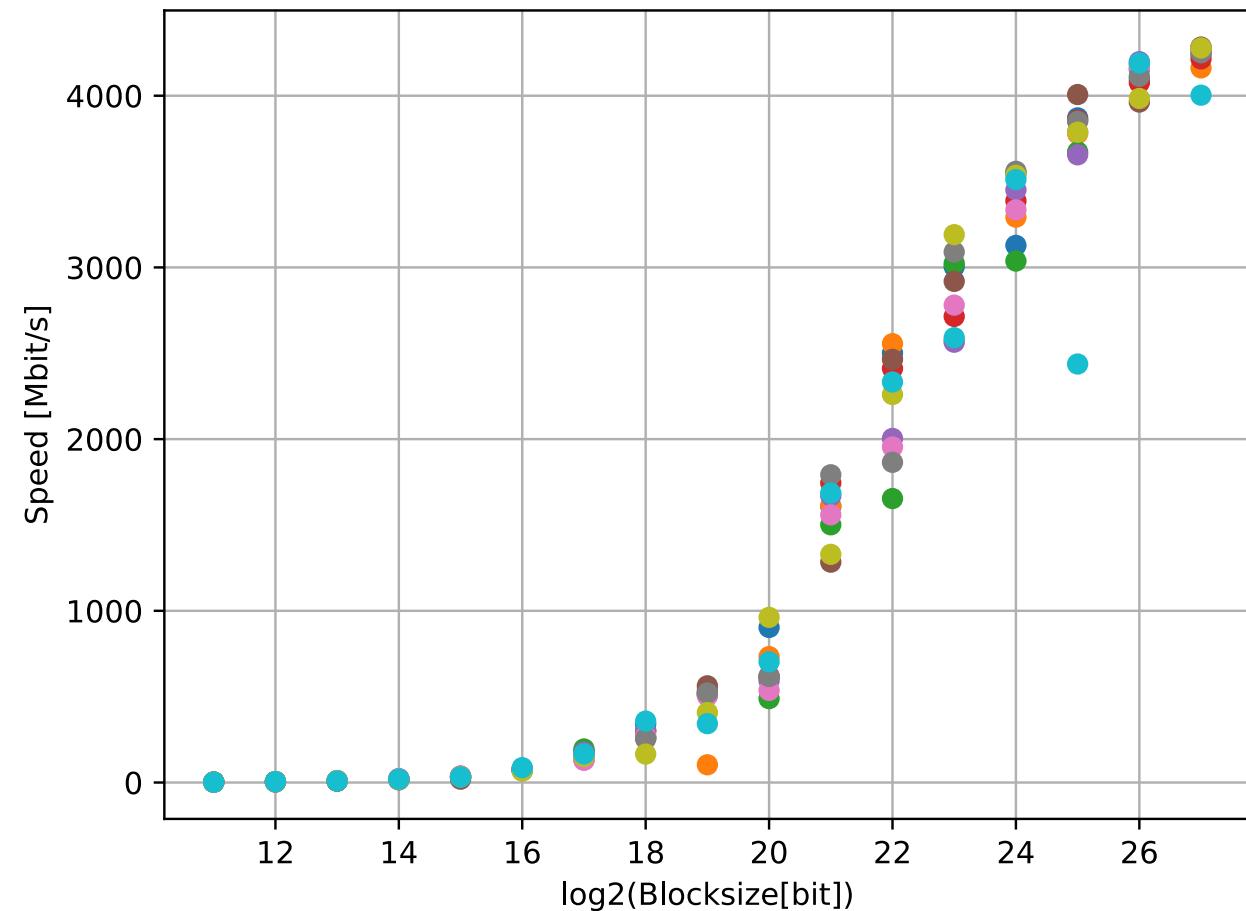
```
1741 -             vuda::launchKernel("SPIRV/binInt2float.spv", "main", BinInt2floatSeedStream, (int)((int)(sample_size)+1023) / 1024), min_template(sample_size, 1024), toeplitz_seed + input_cache_block_size * input_cache_read_pos_seed, di2, count_one_of_global_seed, float1_reduced_dev);
1744 +             vuda::launchKernel("SPIRV/binInt2float.spv", "main", BinInt2floatSeedStream, (int)((int)(sample_size)+1023) / 1024), min_template(sample_size, 1024), toeplitz_seed[input_cache_read_pos_seed], di2, count_one_of_global_seed, float1_reduced_dev);
```

Function	Cuda	Vulkan	Differnece	Differnece %
			Vulkan - Cuda	((Vu/Cu)*100)-100
wait_for_input_buffer [ms]	0.006	0.006	0	0
cleaned_memory [ms]	0.003	0	-0.003	-100 %
set_count_to_zero [ms]	0.007	0.172	0.165	2'357 %
binIntffloat_seed [ms]	2.782	3.043	0.261	9 %
binIntffloat_key [ms]	1.762	1.991	0.229	13 %
calculateCorrectionFloat [ms]	0.068	0.226	0.158	232 %
fft_key [ms]	7.225	6.283	-0.942	-13 %
fft_seed [ms]	7.425	6.638	-0.787	-11 %
setFirstElementToZero [ms]	0.094	0	-0.094	-100 %
elementWiseProduct [ms]	2.397	2.467	0.07	3 %
ifft [ms]	7.352	6.65	-0.702	-10 %
wait_for_output_buffer [ms]	0.005	0.003	-0.002	-40 %
toBinaryArray [ms]	1.725	1.612	-0.113	-7 %
Total [ms]	30.868	29.094	-1.774	-6 %
Speed [MBit/s]	4348.055	4613.213	265.158	6 %

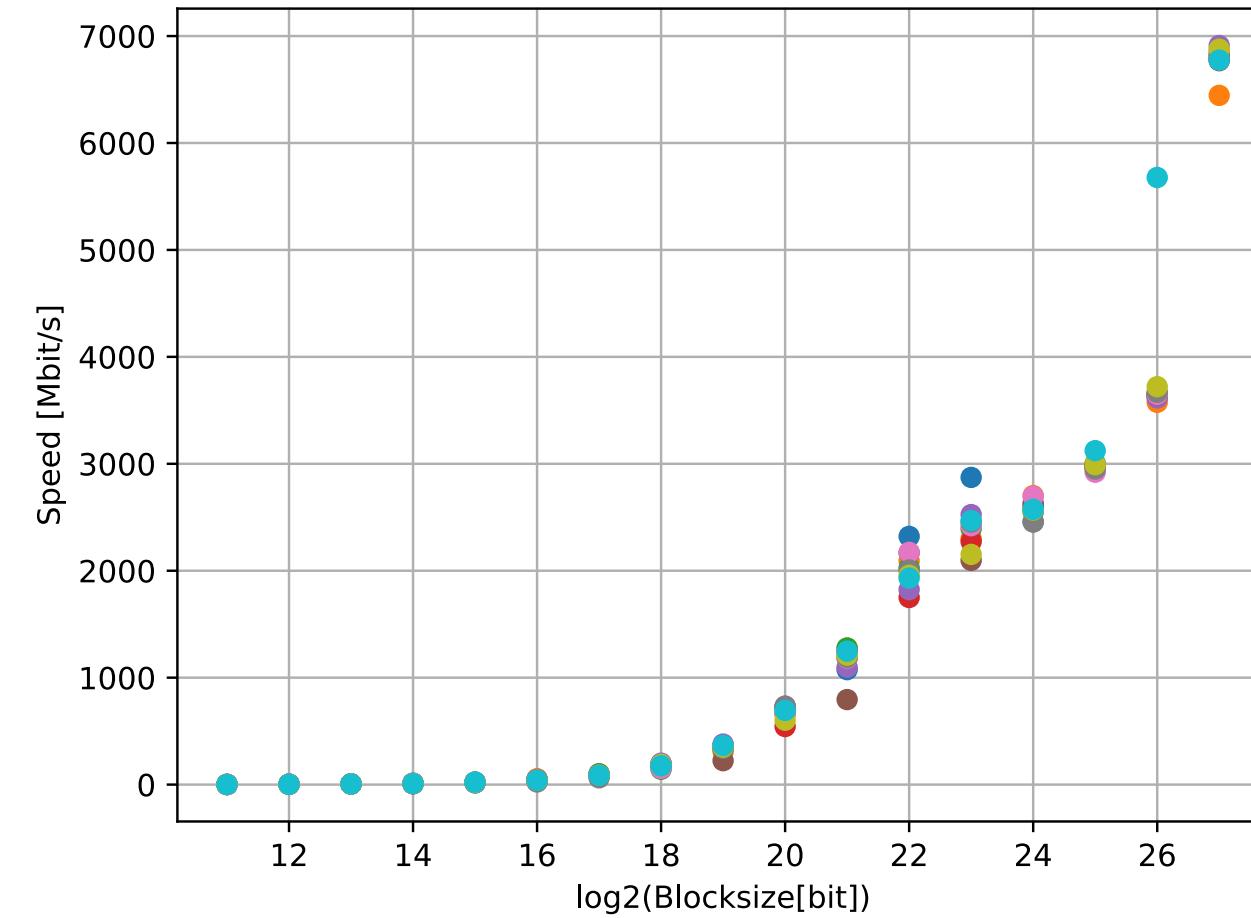
Privacy Amplification Vulkan - RTX 3080 - dynamic Toeplitz seed



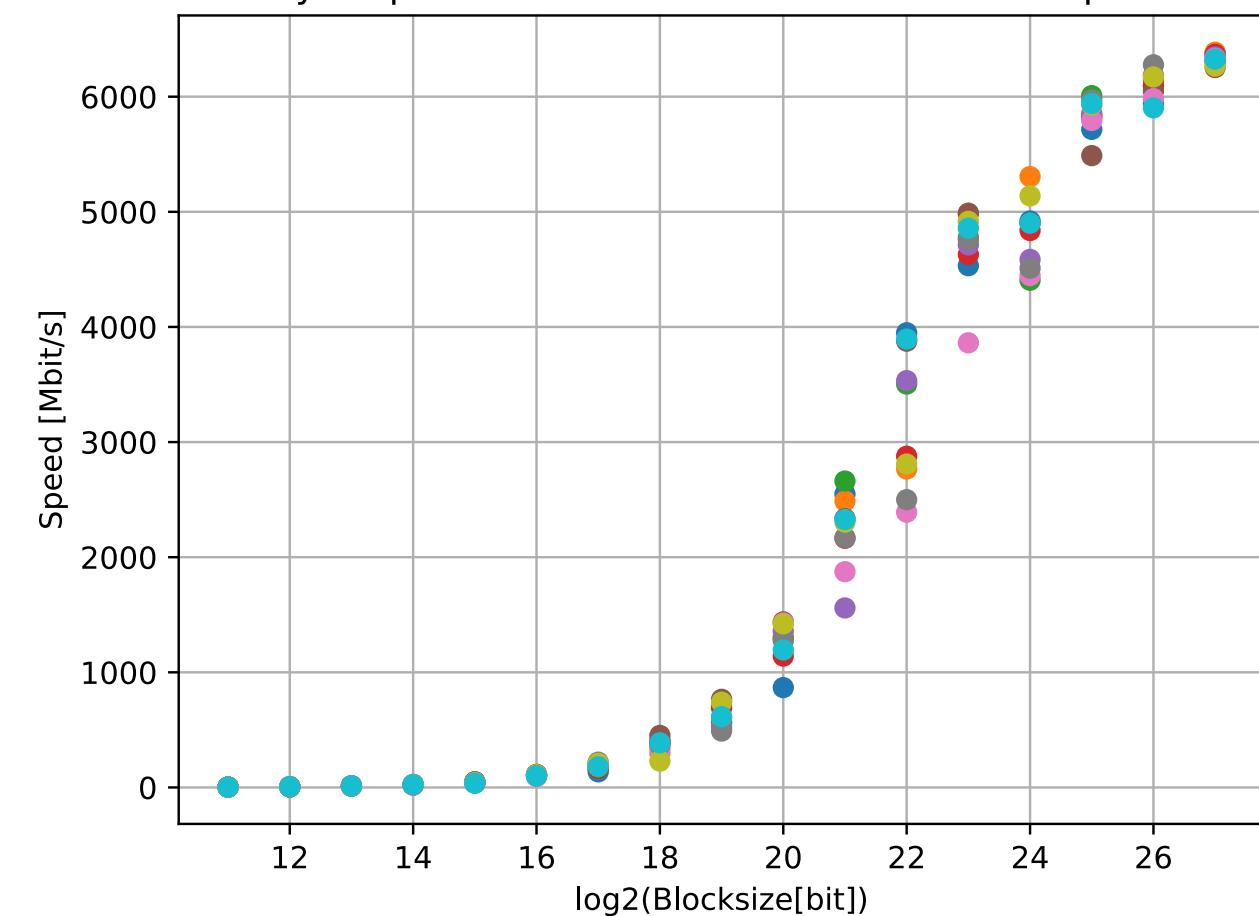
Privacy Amplification Cuda - RTX 3080 - dynamic Toeplitz seed



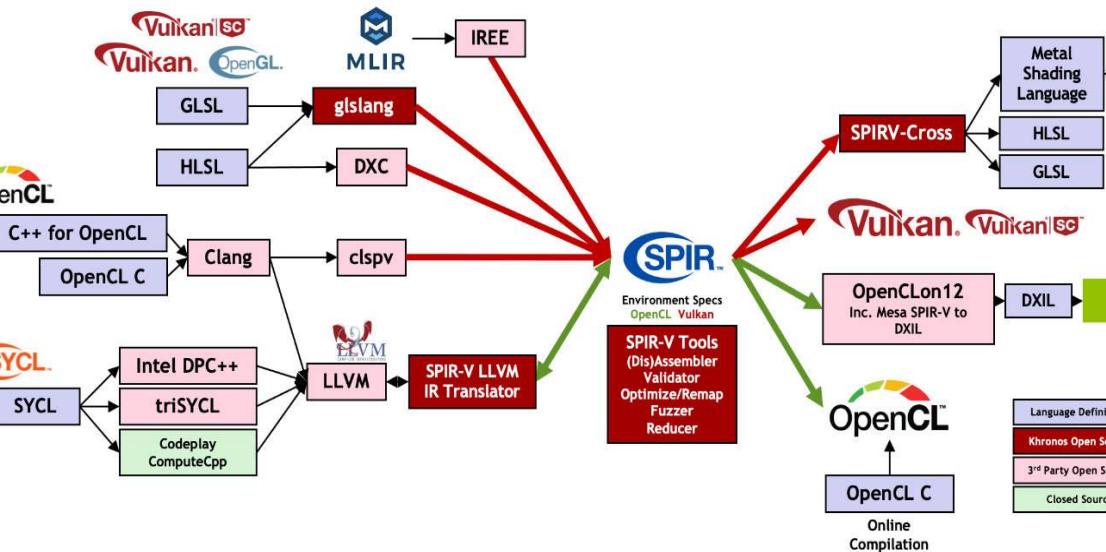
Privacy Amplification Vulkan - RTX 3080 - static Toeplitz seed



Privacy Amplification Cuda - RTX 3080 - static Toeplitz seed



Function	Cuda	Vulkan	Differnece	Differnece %
			Vulkan - Cuda	((Vu/Cu)*100)-100
wait_for_input_buffer [ms]	0.006	0.006	0	0
cleaned_memory [ms]	0.003	0	-0.003	-100 %
set_count_to_zero [ms]	0.007	0.172	0.165	2'357 %
binIntffloat_seed [ms]	2.782	3.043	0.261	9 %
binIntffloat_key [ms]	1.762	1.991	0.229	13 %
calculateCorrectionFloat [ms]	0.068	0.226	0.158	232 %
fft_key [ms]	7.225	6.283	-0.942	-13 %
fft_seed [ms]	7.425	6.638	-0.787	-11 %
setFirstElementToZero [ms]	0.094	0	-0.094	-100 %
elementWiseProduct [ms]	2.397	2.467	0.07	3 %
ifft [ms]	7.352	6.65	-0.702	-10 %
wait_for_output_buffer [ms]	0.005	0.003	-0.002	-40 %
toBinaryArray [ms]	1.725	1.612	-0.113	-7 %
Total [ms]	30.868	29.094	-1.774	-6 %
Speed [MBit/s]	4348.055	4613.213	265.158	6 %



PRIVACY AMPLIFICATION

