

DPDK Intel Cryptodev Performance Report Release 18.11

Test Date: November 29th 2018

Author: Intel DPDK Validation team



Revision History

Date	Revision	Comment
November 29th, 2018	1.0	Initial document for release



Contents

Audience and Purpose	4
Test setup:	4
Intel® Xeon® Platinum 8180 Processor (38.5M Cache, 2.50 GHz)	6 7
Intel® Xeon® Processor D-1553N (12M Cache, 2.30 GHz)	11 12
Intel Atom® Processor C3958 (16M Cache, 2.00 GHz)	15 15



Audience and Purpose

The primary audience for this test report are architects and engineers implementing the Data Plane Development Kit (DPDK). This report provides information on packet processing performance testing for the specified DPDK release on Intel® architecture. The initial report may be viewed as the baseline for future releases and provides system configuration and test cases based on DPDK examples.

The purpose of reporting these tests is not to imply a single "correct" approach, but rather to provide a baseline of well-tested configurations and procedures with reproducible results. This will help guide architects and engineers who are evaluating and implementing DPDK solutions on Intel® architecture and can assist in achieving optimal system performance.

Test setup:

The device under test (DUT) consists of a system with an Intel® architecture motherboard populated with the following;

- A single or dual processor and PCH chip, except for System on Chip (SoC) cases
- DRAM memory size and frequency (normally single DIMM per channel)
- Specific Intel Network Interface Cards (NICs)
- BIOS settings noting those that updated from the basic settings
- DPDK build configuration settings, and commands used for tests

Benchmarking a DPDK system requires knowledge of networking technologies including knowledge of network protocols and hands-on experience with relevant open-source software, such as Linux*, and the DPDK. Engineers also need benchmarking and debugging skills, as well as a good understanding of the device-under-test (DUT) across compute and networking domains.

dpdk-test-crypto-perf Application: Documentation may be found at http://dpdk.org/doc/quides/tools/cryptoperf.html.

The dpdk-test-crypto-perf tool is a Data Plane Development Kit (DPDK) utility that allows measuring performance parameters of PMDs available in the crypto tree. There are available for two measurement types: throughput and latency. Users can use multiple cores to run tests on but only one type of crypto PMD can be measured during single application execution. Cipher parameters, type of device, type of operation and chain mode have to be specified in the command line as application parameters. These parameters are checked using device capabilities structure.

Below is an example setup topology for the performance test. Generally, Cores, memories, Intel QuickAssist Technology hardware are connected to same socket. The performance result for multi-core testing sums each core's throughput number.



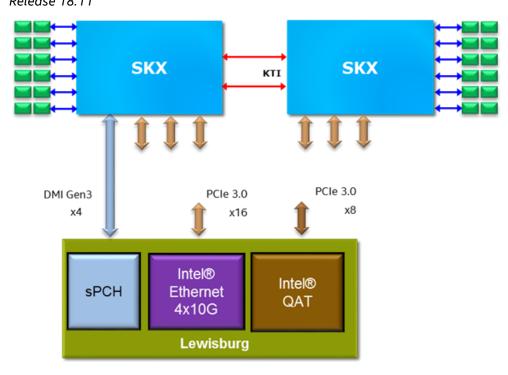


Figure 1. DPDK cryptodev performance test setup



Intel® Xeon® Platinum 8180 Processor (38.5M Cache, 2.50 GHz)

Hardware & Software Ingredients

naraware a software ingredients		
Item	Description	
Server Platform	PURLEY	
Chipset	Intel® C620 Series Chipset	
CPU	Intel(R) Xeon(R) Platinum 8180 CPU @ 2.50GHz	
	https://ark.intel.com/products/120496/Intel-Xeon-Platinum-8180-Processor-38 5M-Cache-2 50-GHz	
	Number of cores 28, Number of threads 56.	
Memory	Total 98304 MBs over 12 channels @ 2133 MHz	
PCIe	3 x PCIe Gen3 x8 slots	
QAT	PCI-e x16 mode	
Operating System	Ubuntu16.04	
BIOS	SE5C620.86B.00.01.0009.101920170742	
Microcode version	0x2000030	
Linux kernel version	4.13.0-36-generic	
GCC version	5.4.0 20160609	
DPDK version	18.11	

Boot and BIOS settings

Boot and Bros sectings		
Item	Description	
Boot settings	<pre>intel_iommu=on iommu=pt intel_pstate=disable isolcpus=6-15,22-31 nohz_full=6-15,22-31 rcu_nocbs=6-15,22-31</pre>	
BIOS	CPU Power and Performance Policy <performance> CPU C-state Disabled CPU P-state Disabled Enhanced Intel® Speedstep® Tech Disabled Turbo Boost Disabled</performance>	
DPDK Settings	Build Options: config/common_base CONFIG_RTE_LIBRTE_PMD_QAT_SYM=y CONFIG_RTE_LIBRTE_PMD_AESNI_MB=y CONFIG_RTE_LIBRTE_PMD_AESNI_GCM=y	



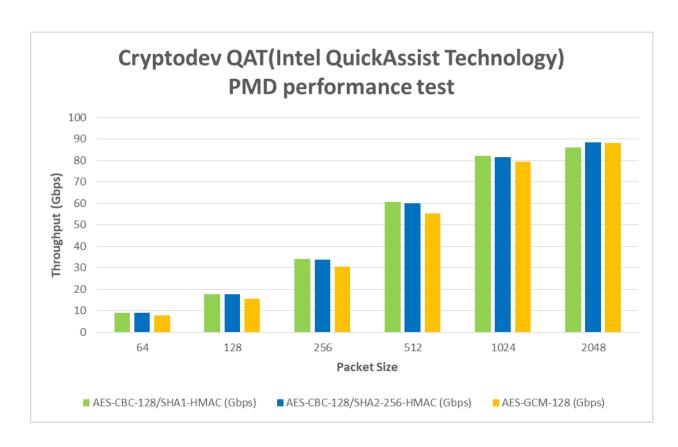
Test Case 1 – Cryptodev QAT(Intel QuickAssist Technology) PMD performance test

Itam	Description	
Item Test Case	Description Cryptodev performance for AES-CBC-128/SHA1-HMAC, AES-GCM-128, AES-CBC-	
rest case	128/SHA2-256-HMAC with Intel QuickAssist Technology	
Cores	3C6T	
QAT	Integrated Intel QuickAssist Technology , PCI-e x16 Mode	
Command line (AES-CBC- 128/SHA1-HMAC)	./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perfsocket-mem 2048,0legacy-mem -w 0000:1a:01.0 -w 0000:1c:01.0 -w 0000:1a:01.0 -w 0000:1a:01.1 -w 0000:1c:01.1 -w 0000:1c:01.1 -w 0000:1a:01.3 -w 0000:1a:01.2 -w 0000:1a:01.2 -w 0000:1a:01.3 -w 0000:1c:01.3 -w 0000:1c:01.3 -w 0000:1a:01.3 -w 0000:1c:01.4 -w 0000:1c:01.4 -w 0000:1c:01.5 -w 0000:1c:01.0 qat_sym,slave=0000:1c:01.0 qat_sym,mode=round-robin vdev=crypto_scheduler_pmd_2,slave=0000:1a:01.1_qat_sym,slave=0000:1c:01.2 qat_sym,slave=0000:1c:01.2 qat_sym,slave=0000:1c:01.2 qat_sym,slave=0000:1c:01.3 qat_sym,slave=0000:1c:01.3 qat_sym,slave=0000:1c:01.3 qat_sym,slave=0000:1c:01.3 qat_sym,slave=0000:1c:01.4 qat_sym,slave=0000:1c:01.4 qat_sym,slave=0000:1c:01.5 qat_sym,slave=0000:	
	-n 6buffer-sz 64,128,256,512,1024,2048optype cipher-then-auth ptest throughputauth-key-sz 64cipher-key-sz 16devtype crypto_schedulercipher-iv-sz 16auth-op generateburst-sz 32 total-ops 30000000silentdigest-sz 20auth-algo shal-hmac cipher-algo aes-cbccipher-op encrypt ./x86 64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-	
Command line (AES-CBC- 128/SHA2-256- HMAC)	perfsocket-mem 2048,0legacy-mem -w 0000:1a:01.0 -w 0000:1c:01.0 -w 0000:1e:01.0 -w 0000:1a:01.1 -w 0000:1c:01.1 -w 0000:1a:01.2 -w 0000:1a:01.2 -w 0000:1c:01.2 -w 0000:1a:01.3 -w 0000:1c:01.3 -w 0000:1c:01.3 -w 0000:1a:01.3 -w 0000:1c:01.3 -w 0000:1a:01.5 -w 0000:1c:01.4 -w 0000:1a:01.4 -w 0000:1a:01.5 -w 0000:1a:01.0 -w 0000:1a:01.0 -w 0000:1a:01.0 -w 0000:1a:01.0 -w 0000:1a:01.0 -w 0000:1a:01.0 -w 0000:1a:01.1 -w 0000:1a:01.1 -w 0000:1a:01.1 -w 0000:1a:01.1 -w 0000:1a:01.1 -w 0000:1a:01.2 -w 0000:1a:01.3 -w 0000:	
Command line (AES-GCM-128)	./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perfsocket-mem 2048,0legacy-mem -w 0000:1a:01.0 -w 0000:1c:01.0 -w 0000:1e:01.0 -w 0000:1a:01.1 -w 0000:1c:01.1 -w 0000:1e:01.1 -w 0000:1a:01.2 -w 0000:1a:01.2 -w 0000:1a:01.2 -w 0000:1a:01.3 -w 0000:1c:01.3 -w 0000:1c:01.3 -w 0000:1c:01.4 -w 0000:1c:01.4 -w 0000:1c:01.5 -vdev crypto_scheduler_pmd_1,slave=0000:1a:01.5 -w 0000:1e:01.5 -vdev crypto_scheduler_pmd_1,slave=0000:1a:01.0_qat_sym,slave=0000:1c:01.0_qat_sym,slave=0000:1c:01.0_qat_sym,slave=0000:1c:01.1_qat_sym,slave=0000:1c:01.1_qat_sym,slave=0000:1c:01.1_qat_sym,slave=0000:1c:01.1_qat_sym,slave=0000:1c:01.1_qat_sym,slave=0000:1c:01.1_qat_sym,slave=0000:1c:01.2_qat_sym,slave=0000:1c:01.2_qat_sym,slave=0000:1c:01.2_qat_sym,slave=0000:1c:01.3_qat_sym,slave=0000:1c:01.3_	



	qat_sym,slave=0000:1e:01.3_qat_sym,mode=round-robin vdev=crypto_scheduler_pmd_5,slave=0000:1a:01.4_qat_sym,slave=0000:1c:01.4_ qat_sym,slave=0000:1e:01.4_qat_sym,mode=round-robin vdev=crypto_scheduler_pmd_6,slave=0000:1a:01.5_qat_sym,slave=0000:1c:01.5_ qat_sym,slave=0000:1e:01.5_qat_sym,mode=round-robin -1 9,10,66,11,67,12,68 -n 6aead-key-sz 16buffer-sz 64,128,256,512,1024,2048optype aeadptest throughputaead-aad-sz 16devtype crypto_scheduler aead-op encryptburst-sz 32total-ops 30000000silentdigest-sz 16aead-algo aes-gcmaead-iv-sz 12
Notes	Use multi-cores configuration for testing is aim to reach maximum of QAT capability

Buffer Size	AES-CBC-128/SHA1-HMAC	AES-CBC-128/SHA2-256-HMAC	AES-GCM-128
(Bytes)	(Gbps)	(Gbps)	(Gbps)
64	9.03	8.98	7.91
128	17.78	17.68	15.72
256	34.25	34.06	30.59
512	60.66	60.78	55.53
1024	82.24	82.55	79.98
2048	85.80	88.72	88.38



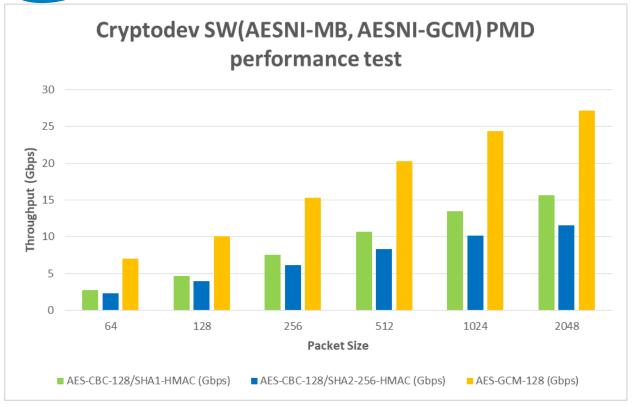


Test Case 2 – Cryptodev SW (AESNI-MB, AESNI-GCM) PMD performance test

Item	Description	
Test Case	Cryptodev performance for AES-CBC-128/SHA1-HMAC, AES-GCM-128, AES-CBC-128/SHA2-256-HMAC, KASUMI-F8/KASUMI-F9, SNOW3G-UEA2/SNOW3G-UIA2, ZUC-EEA3/ZUC-EIA3	
Cores	1C1T	
QAT	Not use	
Command line (AES-CBC- 128/SHA1-HMAC)	./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perfsocket-mem 2048,0legacy-memvdev crypto_aesni_mb_pmd_1 -1 9,10 -n 6buffer-sz 64,128,256,512,1024,2048optype cipher-then-authptest throughputauth-key-sz 64cipher-key-sz 16devtype crypto_aesni_mbcipher-iv-sz 16auth-op generateburst-sz 32total-ops 10000000silentdigest-sz 12auth-algo shal-hmaccipher-algo aes-cbccipher-op encrypt	
Command line (AES-CBC- 128/SHA2-256- HMAC)	./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perfsocket-mem 2048,0legacy-memvdev crypto_aesni_mb_pmd_1 -1 9,10 -n 6buffer-sz 64,128,256,512,1024,2048optype cipher-then-authptest throughputauth-key-sz 64cipher-key-sz 16devtype crypto_aesni_mbcipher-iv-sz 16auth-op generateburst-sz 32total-ops 10000000silentdigest-sz 16auth-algo sha2-256-hmaccipher-algo aes-cbccipher-op encrypt	
Command line (AES-GCM-128)	./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perfsocket-mem 2048,0legacy-memvdev crypto_aesni_gcm_pmd_1 -1 9,10 -n 6aead-key-sz 16buffer-sz 64,128,256,512,1024,2048 optype aeadptest throughputaead-aad-sz 16devtype crypto_aesni_gcmaead-op encryptburst-sz 32total-ops 10000000silentdigest-sz 16aead-algo aes-gcmaead-iv-sz 12	
Notes	The SW PMD performance is linear scaling out with core numbers.	
	The scale factor is around 1. If the hyper-threading is enabled, extra ~20%-50%	
	performance will be achieved per hyper-thread.	

Buffer Size	AES-CBC-128/SHA1-HMAC	AES-CBC-128/SHA2-256-HMAC	AES-GCM-128
(Bytes)	(Gbps)	(Gbps)	(Gbps)
64	2.87	2.27	6.88
128	4.91	3.86	9.99
256	7.77	5.96	15.20
512	10.90	8.21	20.15
1024	13.66	10.09	24.25
2048	15.70	11.45	27.08







Intel® Xeon® Processor D-1553N (12M Cache, 2.30 GHz)

Hardware & Software Ingredients

Item	Description
Server Platform	GRANGEVILLE
CPU	Intel® Xeon® Processor D-1553N (12M Cache, 2.30 GHz)
	https://ark.intel.com/products/123002/Intel-Xeon-Processor-D-1553N-12M- Cache-2 30-GHz
	Number of cores 8, Number of threads 16.
Memory	Total 65536 MBs over 4 channels @ 2400 MHz
Operating System	Ubuntu 16.04
BIOS	GNVDTRL1.86B.0010.D51.1706230411
Microcode version	0xe000004
Linux kernel version	4.13.0-36-generic
GCC version	5.4.0 20160609
DPDK version	18.11

Boot and BIOS settings

Item	Description	
Boot settings	<pre>intel_iommu=on iom mu=pt intel_pstate=disable isolcpus=4-7,12-15 nohz_full=4-7,12-15 rcu_nocbs=4-7,12-15 hugepagesz=1G hugepages=10 default_hugepagesz=1G</pre>	
BIOS	CPU Power and Performance Policy < Performance >	
	CPU C-state Disabled CPU P-state Disabled	
	Enhanced Intel® Speedstep® Tech Disabled	
	Turbo Boost Disabled	
DPDK Settings	Build Options: config/common_base	
	CONFIG_RTE_LIBRTE_PMD_QAT_SYM=y	
	CONFIG_RTE_LIBRTE_PMD_AESNI_MB=y	
	CONFIG_RTE_LIBRTE_PMD_AESNI_GCM=y	

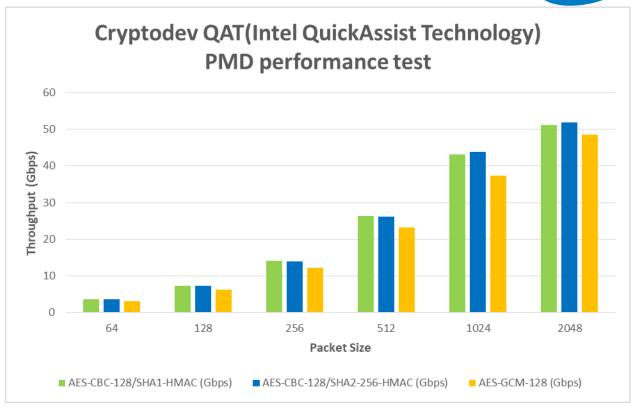


Test Case 3 – Cryptodev QAT(Intel QuickAssist Technology) PMD performance test

Item	Description	
Test Case	Cryptodev performance for AES-CBC-128/SHA1-HMAC, AES-GCM-128, AES-CBC-128/SHA2-256-HMAC by Intel QuickAssist Technology	
Cores	2C4T	
QAT	Integrated Intel QuickAssist Technology	
Command line (AES-CBC- 128/SHA1-HMAC)	./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perfsocket-mem 2048,0legacy-mem -w 0000:02:01.0 -w 0000:02:01.1 -w 0000:02:01.2 -w 0000:02:01.3 -1 4,5,13,6,14 -n 4buffer-sz 64,128,256,512,1024,2048optype cipher-then-authptest throughput auth-key-sz 64cipher-key-sz 16devtype crypto_gatcipher-iv-sz 16 auth-op generateburst-sz 32total-ops 30000000silentdigest-sz 20auth-algo shal-hmaccipher-algo aes-cbccipher-op encrypt	
Command line (AES-CBC- 128/SHA2-256- HMAC)	./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perfsocket-mem 2048,0legacy-mem -w 0000:02:01.0 -w 0000:02:01.1 -w 0000:02:01.2 -w 0000:02:01.3 -l 4,5,13,6,14 -n 4buffer-sz 64,128,256,512,1024,2048optype cipher-then-authptest throughput auth-key-sz 64cipher-key-sz 16devtype crypto_gatcipher-iv-sz 16auth-op generateburst-sz 32total-ops 30000000silentdigest-sz 32auth-algo sha2-256-hmaccipher-algo aes-cbccipher-op encrypt	
Command line (AES-GCM-128)	./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perfsocket-mem 2048,0legacy-mem -w 0000:02:01.0 -w 0000:02:01.1 -w 0000:02:01.2 -w 0000:02:01.3 -l 4,5,13,6,14 -n 4aead-key-sz 16buffer-sz 64,128,256,512,1024,2048optype aeadptest throughputaead-aad-sz 16devtype crypto_qataead-op encryptburst-sz 32total-ops 30000000silentdigest-sz 16aead-algo aes-gcmaead-iv-sz 12	
Notes	Use multi-cores configuration for testing is aim to reach maximum of QAT capability	

Buffer Size(Bytes)	AES-CBC-128/SHA1-HMAC	AES-CBC-128/SHA2-256-HMAC	AES-GCM-128
	(Gbps)	(Gbps)	(Gbps)
64	3.71	3.70	3.18
128	7.27	7.25	6.29
256	14.04	13.94	12.33
512	26.35	26.06	23.12
1024	43.06	43.75	37.24
2048	51.07	51.46	48.32





Test Case 4 – Cryptodev SW (AESNI-MB, AESNI-GCM) PMD performance test

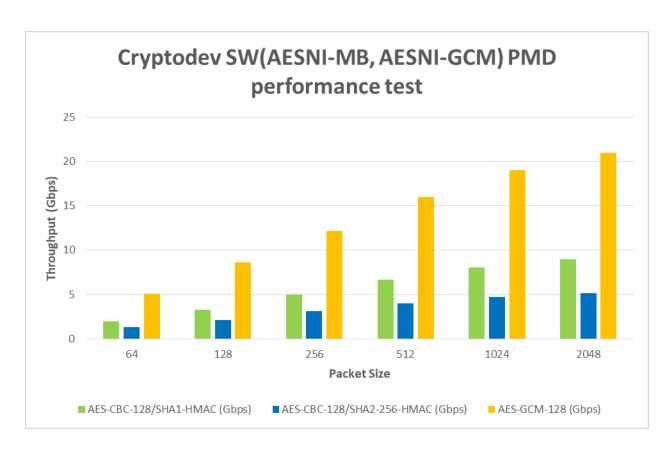
Item	Description		
Test Case	Cryptodev performance for AES-CBC-128/SHA1-HMAC, AES-GCM-128, AES-CBC-128/SHA2-256-HMAC		
Cores	1C1T		
QAT	Not use		
Command line (AES-CBC- 128/SHA1-HMAC)	./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perfsocket-mem 2048,0legacy-memvdev crypto_aesni_mb_pmd_1 -1 4,5 -n 4buffer-sz 64,128,256,512,1024,2048optype cipher-then-authptest throughputauth-key-sz 64cipher-key-sz 16devtype crypto_aesni_mbcipher-iv-sz 16auth-op generateburst-sz 32total-ops 10000000silentdigest-sz 12auth-algo shal-hmaccipher-algo aes-cbccipher-op encrypt		
Command line (AES-CBC- 128/SHA2-256- HMAC)	./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perfsocket-mem 2048,0legacy-memvdev crypto_aesni_mb_pmd_1 -1 4,5 -n 4buffer-sz 64,128,256,512,1024,2048optype cipher-then-authptest throughputauth-key-sz 64cipher-key-sz 16devtype crypto_aesni_mbcipher-iv-sz 16auth-op generateburst-sz 32total-ops 10000000silentdigest-sz 16auth-algo sha2-256-hmaccipher-algo aes-cbccipher-op encrypt		
Command line (AES-GCM-128)	./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perfsocket-mem 2048,0legacy-memvdev crypto_aesni_gcm_pmd_1 -1 4,5 -n 4aead-key-sz 16buffer-sz 64,128,256,512,1024,2048optype aeadptest throughputaead-aad-sz 16devtype crypto_aesni_gcm aead-op encryptburst-sz 32total-ops 10000000silentdigest-sz 16aead-algo aes-gcmaead-iv-sz 12		
Notes	The SW PMD performance is linear scaling out with core numbers.		
	The scale factor is around 1. If the hyper-threading is enabled, extra ~20%-50%		



performance will be achieved per hyper-thread.

Notes: These tests are running with AESNI MB 0.49, since there is a performance issue with AESNI MB 0.48 on this platform.

Buffer Size	AES-CBC-128/SHA1-HMAC	AES-CBC-128/SHA2-256-HMAC	AES-GCM-128
(Bytes)	(Gbps)	(Gbps)	(Gbps)
64	2.10	1.38	4.98
128	3.47	2.23	8.53
256	5.17	3.19	12.08
512	6.85	4.08	15.94
1024	8.18	4.75	18.98
2048	9.07	5.13	20.97





Intel Atom® Processor C3958 (16M Cache, 2.00 GHz)

Hardware & Software Ingredients

Item	Description		
Server Platform	Harcuvar		
CPU	Intel Atom® Processor C3958 (16M Cache, 2.00 GHz)		
	https://ark.intel.com/products/series/97941/Intel-Atom-Processor-C-Series		
	Number of cores 16, Number of threads 16.		
Memory	Total 8192 MBs over 2 channels @ 2400 MHz		
Operating System	Ubuntu 16.04		
BIOS	HAVLCRB1.X64.0015.D73.1711010409		
Microcode version	0x1c		
Linux kernel version	4.13.0-36-generic		
GCC version	5.4.0 20160609		
DPDK version	18.11		

Boot and BIOS settings

Boot and Bros settings			
Item	Description		
Boot settings	<pre>intel_iommu=on iommu=pt intel_pstate=disable isolcpus=8-15 nohz_full=4-11 rcu_nocbs=1-11 hugepagesz=1G hugepages=40 default_hugepagesz=1G</pre>		
BIOS	CPU Power and Performance Policy <performance> CPU C-state Disabled CPU P-state Disabled Enhanced Intel® Speedstep® Tech Disabled Turbo Boost Disabled</performance>		
DPDK Settings	Build Options: config/common_base CONFIG_RTE_LIBRTE_PMD_QAT_SYM=y CONFIG_RTE_LIBRTE_PMD_AESNI_MB=y CONFIG_RTE_LIBRTE_PMD_AESNI_GCM=y		

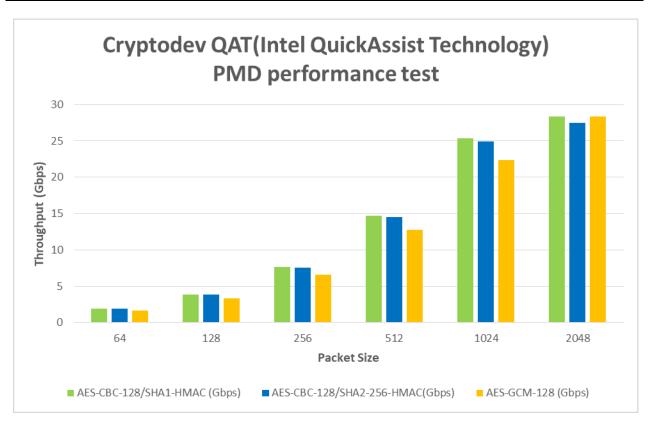
Test Case 5 – Cryptodev QAT(Intel QuickAssist Technology) PMD performance test

Item	Description		
Test Case	Cryptodev performance for AES-CBC-128/SHA1-HMAC, AES-GCM-128, AES-CBC-128/SHA2-256-HMAC by Intel QuickAssist Technology		
Cores	4C4T		
QAT	Integrated Intel QuickAssist Technology		
Command line	./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perfsocket-mem 2048,0legacy-mem -w 0000:01:01.0 -w 0000:01:01.1 -w		
(AES-CBC- 128/SHA1-HMAC)	0000:01:01.2 -w 0000:01:01.3 -1 6,7,8,9,10 -n 2buffer-sz 64,128,256,512,1024,2048optype cipher-then-authptest throughput		



	auth-key-sz 64cipher-key-sz 16devtype crypto_qatcipher-iv-sz 16auth-op generateburst-sz 32total-ops 3000000silentdigest-sz 20auth-algo shal-hmaccipher-algo aes-cbccipher-op encrypt
Command line (AES-CBC- 128/SHA2-256- HMAC)	./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perfsocket-mem 2048,0legacy-mem -w 0000:01:01.0 -w 0000:01:01.1 -w 0000:01:01.2 -w 0000:01:01.3 -1 6,7,8,9,10 -n 2buffer-sz 64,128,256,512,1024,2048optype cipher-then-authptest throughput auth-key-sz 64cipher-key-sz 16devtype crypto_qatcipher-iv-sz 16auth-op generateburst-sz 32total-ops 30000000silentdigest-sz 32auth-algo sha2-256-hmaccipher-algo aes-cbccipher-op encrypt
Command line (AES-GCM-128)	./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perfsocket-mem 2048,0legacy-mem -w 0000:01:01.0 -w 0000:01:01.1 -w 0000:01:01.2 -w 0000:01:01.3 -l 6,7,8,9,10 -n 2aead-key-sz 16 buffer-sz 64,128,256,512,1024,2048optype aeadptest throughput aead-aad-sz 16devtype crypto_qataead-op encryptburst-sz 32 total-ops 30000000silentdigest-sz 16aead-algo aes-gcmaead-iv-sz 12
Notes	Use multi-cores configuration for testing is aim to reach maximum of QAT capability

Test nessarer			
Buffer Size	AES-CBC-128/SHA1-HMAC	AES-CBC-128/SHA2-256-HMAC	AES-GCM-128
(Bytes)	(Gbps)	(Gbps)	(Gbps)
64	1.94	1.93	1.66
128	3.86	3.84	3.32
256	7.62	7.57	6.58
512	14.67	14.55	12.79
1024	25.32	24.92	22.33
2048	28.34	27.49	28.33



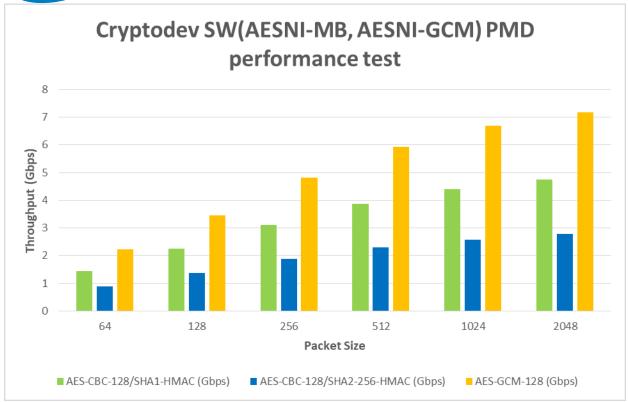


Test Case 6 – Cryptodev SW (AESNI-MB, AESNI-GCM) PMD performance test

Item	Description		
Test Case	Cryptodev performance for AES-CBC-128/SHA1-HMAC, AES-GCM-128, AES-CBC-		
	128/SHA2-256-HMAC		
Cores	1C1T		
QAT	Not use		
Command line (AES-CBC- 128/SHA1-HMAC)	./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perfsocket-mem 2048,0legacy-memvdev crypto_aesni_mb_pmd_1 -1 6,7 -n 2buffer-sz 64,128,256,512,1024,2048optype cipher-then-authptest throughputauth-key-sz 64cipher-key-sz 16devtype crypto_aesni_mbcipher-iv-sz 16auth-op generateburst-sz 32total-ops 10000000silentdigest-sz 12auth-algo shal-hmaccipher-algo aes-cbccipher-op encrypt		
Command line (AES-CBC- 128/SHA2-256- HMAC)	./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perfsocket-mem 2048,0legacy-memvdev crypto_aesni_mb_pmd_1 -1 6,7 -n 2buffer-sz 64,128,256,512,1024,2048optype cipher-then-authptest throughputauth-key-sz 64cipher-key-sz 16devtype crypto_aesni_mbcipher-iv-sz 16auth-op generateburst-sz 32total-ops 10000000silentdigest-sz 16auth-algo sha2-256-hmaccipher-algo aes-cbccipher-op encrypt		
Command line (AES-GCM-128)	./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perfsocket-mem 2048,0legacy-memvdev crypto_aesni_gcm_pmd_1 -l 6,7 -n 2aead-key-sz 16buffer-sz 64,128,256,512,1024,2048optype aeadptest throughputaead-aad-sz 16devtype crypto_aesni_gcm aead-op encryptburst-sz 32total-ops 10000000silentdigest-sz 16aead-algo aes-gcmaead-iv-sz 12		
Notes	The SW PMD performance is linear scaling out with core numbers. The scale factor is around 1.		

rest nesurt.			
Buffer Size	AES-CBC-128/SHA1-HMAC	AES-CBC-128/SHA2-256-HMAC	AES-GCM-128
(Bytes)	(Gbps)	(Gbps)	(Gbps)
64	1.38	0.87	2.22
128	2.19	1.35	3.47
256	3.05	1.85	4.80
512	3.83	2.27	5.91
1024	4.38	2.58	6.68
2048	4.73	2.76	7.16





DPDK Performance Report Release 18.11



DISCLAIMERS

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein.

Tests document performance of components on a particular test, in specific systems. Differences in hardware, software, or configuration will affect actual performance. Consult other sources of information to evaluate performance as you consider your purchase. For more complete information about performance and benchmark results, visit www.intel.com/benchmarks.

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.

Performance results are based on testing as of Nov. 29 and may not reflect all publicly available security updates. See configuration disclosure for details. No product can be absolutely secure. For more information go to http://www.intel.com/performance

Intel® AES-NI requires a computer system with an AES-NI enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on select Intel® processors. For availability, consult your reseller or system manufacturer. For more information, see http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/

Copyright © 2018 Intel Corporation. All rights reserved.

§