DPDK Intel Cryptodev Performance Report
Release 18.02

Test Date: Feb 28th 2018

Author: Intel DPDK Validation team

Revision History

Date	Revision	Comment
Feb 28th, 2018	1.0	Initial document for release

Contents

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/guides/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.

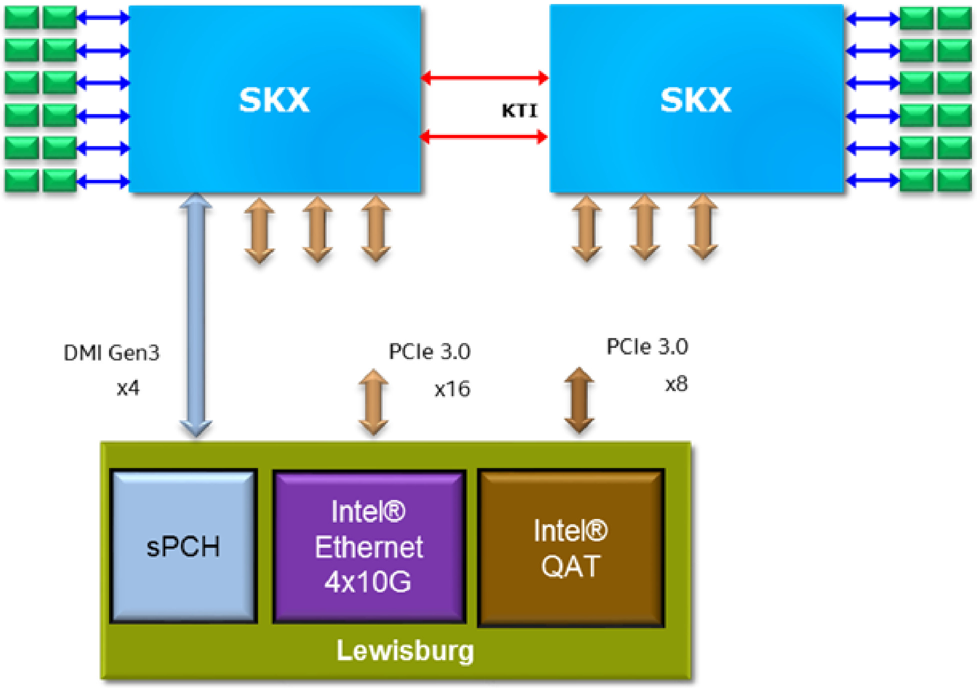


Figure1. DPDK cryptodev performance test setup

Intel® Xeon® Platinum 8176 Processor (38.5M Cache, 2.10 GHz)

Hardware & Software Ingredients

Item	Description
Server Platform	PURLEY
Chipset	Intel® C620 Series Chipset
CPU	Intel® Xeon® Platinum 8176 Processor (38.5M Cache, 2.10 GHz) https://ark.intel.com/products/120508/Intel-Xeon-Platinum-8176-Processor-38_5M-Cache-2_10-GHz Number of cores 28, Number of threads 56. **Notes: Performance Test is running on an engineering prototype that CPU runs at 1.8GHz. On a formal platform should be 2.10GHz, around 10%-20% performance improving is expected.**
Memory	Total 98304 MBs over 12 channels @ 2133 MHz
PCIe	3 x PCIe Gen3 x8 slots
QAT	PCI-e x16 mode
Operating System	Fedora 25
BIOS	PLYDCRB1.86B.0140.R10.1706301640
Linux kernel version	4.8.6-300.fc25.x86_64
GCC version	gcc (GCC) 6.2.1 20160916 (Red Hat 6.2.1-2)
DPDK version	18.02

Boot and BIOS settings

Item	Description
Boot settings	`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`
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=y`
	`CONFIG_RTE_LIBRTE_PMD_AESNI_MB=y`
	`CONFIG_RTE_LIBRTE_PMD_AESNI_GCM=y`

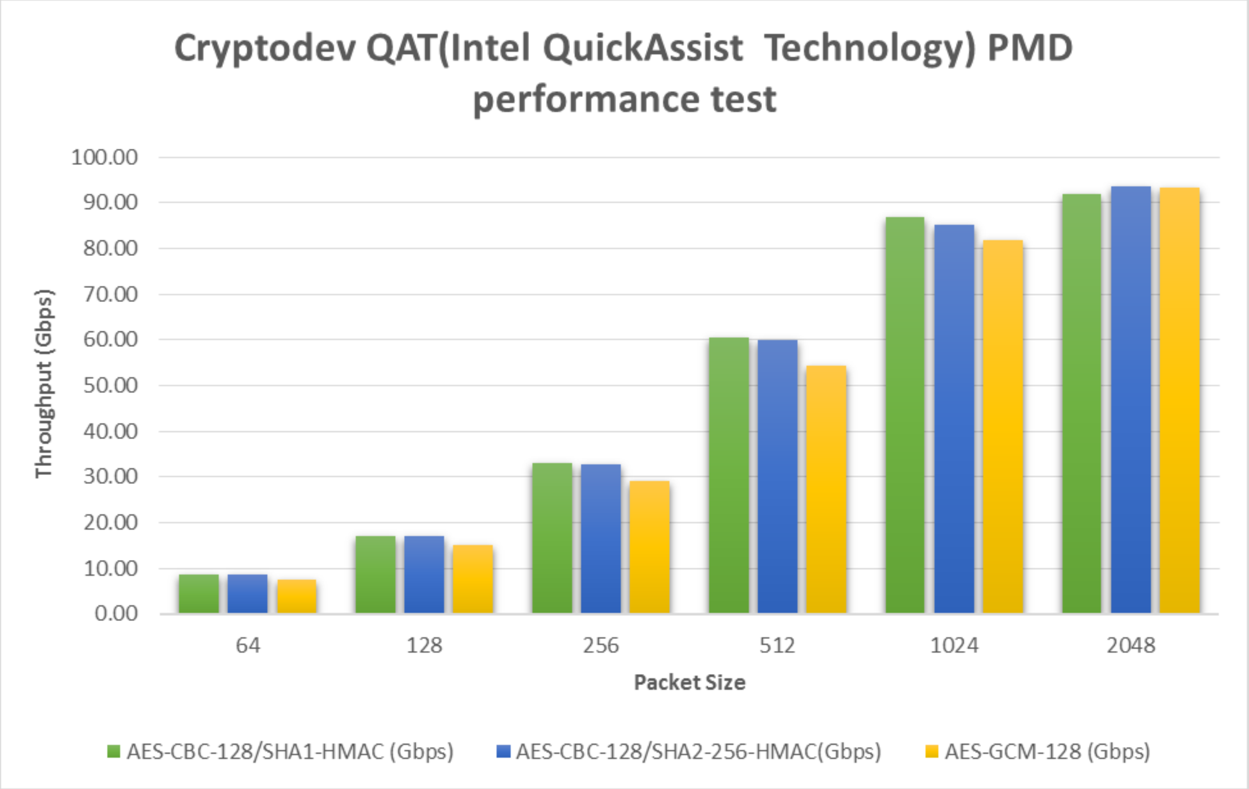
Test Case 1 – Cryptodev QAT(Intel QuickAssist Technology) PMD performance test

Item	Description
Test Case	Cryptodev performance for AES-CBC-128/SHA1-HMAC, AES-GCM-128, AES-CBC-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-perf --socket-mem 2048,0 -w 0000:b9:01.0 -w 0000:b5:01.0 -w 0000:b7:01.0 -w 0000:b9:01.1 -w 0000:b5:01.1 -w 0000:b7:01.1 -w 0000:b9:01.2 -w 0000:b5:01.2 -w 0000:b7:01.2 -w 0000:b9:01.3 -w 0000:b5:01.3 -w 0000:b7:01.3 -w 0000:b9:01.4 -w 0000:b5:01.4 -w 0000:b7:01.4 -w 0000:b9:01.5 -w 0000:b5:01.5 -w 0000:b7:01.5 --vdev crypto_scheduler_pmd_1,slave=0000:b9:01.0,slave=0000:b5:01.0,slave=0000:b7:01.0,mode=round-robin --vdev=crypto_scheduler_pmd_2,slave=0000:b9:01.1,slave=0000:b5:01.1,slave=0000:b7:01.1,mode=round-robin --vdev=crypto_scheduler_pmd_3,slave=0000:b9:01.2,slave=0000:b5:01.2,slave=0000:b7:01.2,mode=round-robin --vdev=crypto_scheduler_pmd_4,slave=0000:b9:01.3,slave=0000:b5:01.3,slave=0000:b7:01.3,mode=round-robin --vdev=crypto_scheduler_pmd_5,slave=0000:b9:01.4,slave=0000:b5:01.4,slave=0000:b7:01.4,mode=round-robin --vdev=crypto_scheduler_pmd_6,slave=0000:b9:01.5,slave=0000:b5:01.5,slave=0000:b7:01.5,mode=round-robin -l 9,10,26,11,27,12,28 -n 6 -- --buffer-sz 64,128,256,512,1024,2048 --optype cipher-then-auth --ptest throughput --auth-key-sz 64 --cipher-key-sz 16 --devtype crypto_scheduler --cipher-iv-sz 16 --auth-op generate --burst-sz 32 --total-ops 30000000 --silent --digest-sz 20 --auth-algo sha1-hmac --cipher-algo aes-cbc --cipher-op encrypt`
Command line (AES-CBC-128/SHA2-256-HMAC)	`./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perf --socket-mem 2048,0 -w 0000:b9:01.0 -w 0000:b5:01.0 -w 0000:b7:01.0 -w 0000:b9:01.1 -w 0000:b5:01.1 -w 0000:b7:01.1 -w 0000:b9:01.2 -w 0000:b5:01.2 -w 0000:b7:01.2 -w 0000:b9:01.3 -w 0000:b5:01.3 -w 0000:b7:01.3 -w 0000:b9:01.4 -w 0000:b5:01.4 -w 0000:b7:01.4 -w 0000:b9:01.5 -w 0000:b5:01.5 -w 0000:b7:01.5 --vdev crypto_scheduler_pmd_1,slave=0000:b9:01.0,slave=0000:b5:01.0,slave=0000:b7:01.0,mode=round-robin --vdev=crypto_scheduler_pmd_2,slave=0000:b9:01.1,slave=0000:b5:01.1,slave=0000:b7:01.1,mode=round-robin --vdev=crypto_scheduler_pmd_3,slave=0000:b9:01.2,slave=0000:b5:01.2,slave=0000:b7:01.2,mode=round-robin --vdev=crypto_scheduler_pmd_4,slave=0000:b9:01.3,slave=0000:b5:01.3,slave=0000:b7:01.3,mode=round-robin --vdev=crypto_scheduler_pmd_5,slave=0000:b9:01.4,slave=0000:b5:01.4,slave=0000:b7:01.4,mode=round-robin --vdev=crypto_scheduler_pmd_6,slave=0000:b9:01.5,slave=0000:b5:01.5,slave=0000:b7:01.5,mode=round-robin -l 9,10,26,11,27,12,28 -n 6 -- --buffer-sz 64,128,256,512,1024,2048 --optype cipher-then-auth --ptest throughput --auth-key-sz 64 --cipher-key-sz 16 --devtype crypto_scheduler --cipher-iv-sz 16 --auth-op generate --burst-sz 32 --total-ops 30000000 --silent --digest-sz 32 --auth-algo sha2-256-hmac --cipher-algo aes-cbc --cipher-op encrypt`
Command line (AES-GCM-128)	`./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perf --socket-mem 2048,0 -w 0000:b9:01.0 -w 0000:b5:01.0 -w 0000:b7:01.0 -w 0000:b9:01.1 -w 0000:b5:01.1 -w 0000:b7:01.1 -w 0000:b9:01.2 -w 0000:b5:01.2 -w 0000:b7:01.2 -w 0000:b9:01.3 -w 0000:b5:01.3 -w 0000:b7:01.3 -w 0000:b9:01.4 -w 0000:b5:01.4 -w 0000:b7:01.4 -w 0000:b9:01.5 -w 0000:b5:01.5 -w 0000:b7:01.5 --vdev crypto_scheduler_pmd_1,slave=0000:b9:01.0,slave=0000:b5:01.0,slave=0000:b7:01.0,mode=round-robin --vdev=crypto_scheduler_pmd_2,slave=0000:b9:01.1,slave=0000:b5:01.1,slave=0000:b7:01.1,mode=round-robin --vdev=crypto_scheduler_pmd_3,slave=0000:b9:01.2,slave=0000:b5:01.2,slave=0000:b7:01.2,mode=round-robin --vdev=crypto_scheduler_pmd_4,slave=0000:b9:01.3,slave=0000:b5:01.3,slave=00`

	`00:b7:01.3,mode=round-robin --vdev=crypto_scheduler_pmd_5,slave=0000:b9:01.4,slave=0000:b5:01.4,slave=0000:b7:01.4,mode=round-robin --vdev=crypto_scheduler_pmd_6,slave=0000:b9:01.5,slave=0000:b5:01.5,slave=0000:b7:01.5,mode=round-robin -l 9,10,26,11,27,12,28 -n 6 -- --aead-key-sz 16 --buffer-sz 64,128,256,512,1024,2048 --optype aead --ptest throughput --aead-aad-sz 16 --devtype crypto_scheduler --aead-op encrypt --burst-sz 32 --total-ops 30000000 --silent --digest-sz 16 --aead-algo aes-gcm --aead-iv-sz 12`
Notes	Use multi-cores configuration for testing is aim to reach maximum of QAT capability

Test Result:

Buffer Size(Bytes)	AES-CBC-128/SHA1-HMAC (Gbps)	AES-CBC-128/SHA2-256-HMAC(Gbps)	AES-GCM-128 (Gbps)
64	8.50	8.46	7.36
128	16.75	16.71	14.58
256	32.60	32.35	28.60
512	60.10	59.50	53.55
1024	86.88	84.90	81.42
2048	91.96	93.73	93.45

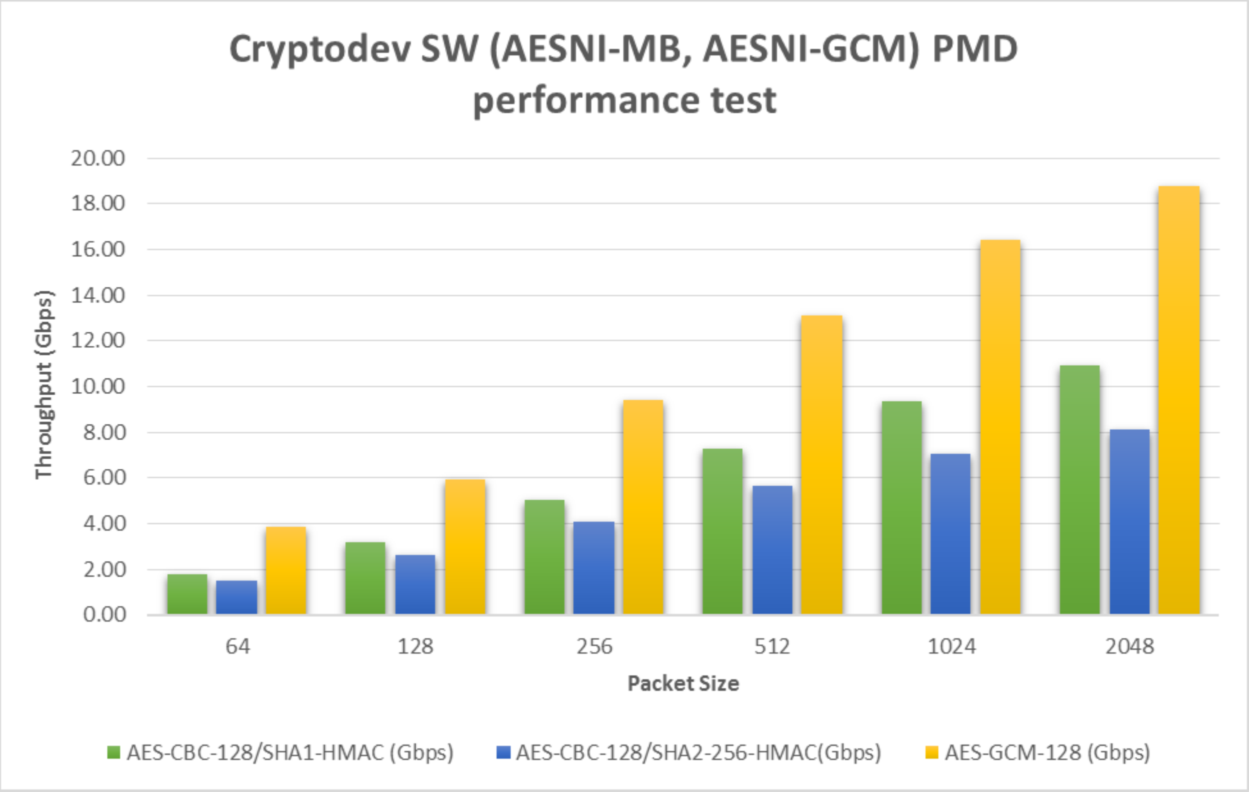


Test Case 2 – Cryptodev SW (AESNI-MB, AESNI-GCM) PMD performance test

Item	Description
Test Case	Cryptodev performance for AES-CBC-128/SHA1-HMAC, AES-GCM-128, AES-CBC-128/SHA2-256-HMAC
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-perf --socket-mem 2048,0 --vdev crypto_aesni_mb_pmd_1 -l 9,10 -n 6 -- --buffer-sz 64,128,256,512,1024,2048 --optype cipher-then-auth --ptest throughput --auth-key-sz 64 --cipher-key-sz 16 --devtype crypto_aesni_mb --cipher-iv-sz 16 --auth-op generate --burst-sz 32 --total-ops 10000000 --silent --digest-sz 12 --auth-algo sha1-hmac --cipher-algo aes-cbc --cipher-op encrypt`
Command line (AES-CBC-128/SHA2-256-HMAC)	`./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perf --socket-mem 2048,0 --vdev crypto_aesni_mb_pmd_1 -l 9,10 -n 6 -- --buffer-sz 64,128,256,512,1024,2048 --optype cipher-then-auth --ptest throughput --auth-key-sz 64 --cipher-key-sz 16 --devtype crypto_aesni_mb --cipher-iv-sz 16 --auth-op generate --burst-sz 32 --total-ops 10000000 --silent --digest-sz 16 --auth-algo sha2-256-hmac --cipher-algo aes-cbc --cipher-op encrypt`
Command line (AES-GCM-128)	`./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perf --socket-mem 2048,0 --vdev crypto_aesni_gcm_pmd_1 -l 9,10 -n 6 -- --aead-key-sz 16 --buffer-sz 64,128,256,512,1024,2048 --optype aead --ptest throughput --aead-aad-sz 16 --devtype crypto_aesni_gcm --aead-op encrypt --burst-sz 32 --total-ops 10000000 --silent --digest-sz 16 --aead-algo aes-gcm --aead-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.

Test Result:

Buffer Size(Bytes)	AES-CBC-128/SHA1-HMAC (Gbps)	AES-CBC-128/SHA2-256-HMAC(Gbps)	AES-GCM-128 (Gbps)
64	1.81	1.52	3.81
128	3.16	2.61	5.91
256	5.03	4.06	9.36
512	7.20	5.63	13.03
1024	9.33	7.02	16.34
2048	10.92	8.08	18.73


Cryptodev SW (AESNI-MB, AESNI-GCM) PMD performance test
Throughput (Gbps)
20.00
18.00
16.00
14.00
12.00
10.00
8.00
6.00
4.00
2.00
0.00
64
128
256
512
1024
2048
Packet Size
🟩 AES-CBC-128/SHA1-HMAC (Gbps)
🟦 AES-CBC-128/SHA2-256-HMAC(Gbps)
🟨 AES-GCM-128 (Gbps)

Intel® Xeon® Processor D-1543N (12M Cache, 2.30 GHz)

Hardware & Software Ingredients

Item	Description
Server Platform	GRANGEVILLE
CPU	Intel® Xeon® Processor D-1543N (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
Linux kernel version	4.10.0-37-generic
GCC version	gcc (Ubuntu 5.4.0-6ubuntu1~16.04.4)
DPDK version	18.02

Boot and BIOS settings

Item	Description
Boot settings	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=1 0 default_hugepagesz=1G
BIOS	CPU Power and Performance Policy <Performance> CPU C-state Disabled CPU P-state Disabled Enhanced Intel® Speedstep® Tech Disabled Turbo Boost Disabled

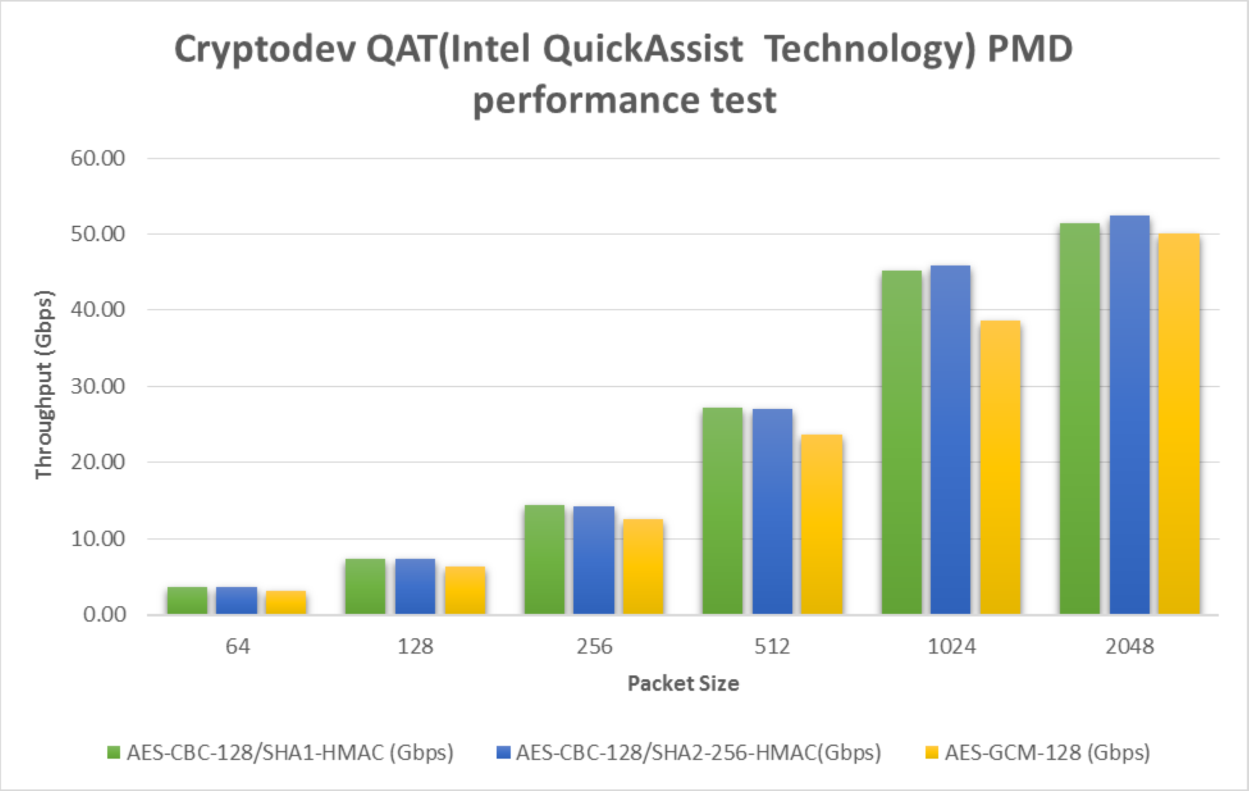
DPDK Settings	Build Options: config/common_base
	CONFIG_RTE_LIBRTE_PMD_QAT=y
	CONFIG_RTE_LIBRTE_PMD_AESNI_MB=y
	CONFIG_RTE_LIBRTE_PMD_AESNI_GCM=y

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-perf --socket-mem 2048,0 -w 0000:02:01.0 -w 0000:02:01.1 -w 0000:02:02.0 -w 0000:02:02.1 -l 4,5,13,6,14 -n 6 -- --buffer-sz 64,128,256,512,1024,2048 --optype cipher-then-auth --ptest throughput --auth-key-sz 64 --cipher-key-sz 16 --devtype crypto_qat --cipher-iv-sz 16 --auth-op generate --burst-sz 32 --total-ops 30000000 --silent --digest-sz 20 --auth-algo sha1-hmac --cipher-algo aes-cbc --cipher-op encrypt`
Command line (AES-CBC-128/SHA2-256-HMAC)	`./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perf --socket-mem 2048,0 -w 0000:02:01.0 -w 0000:02:01.1 -w 0000:02:02.0 -w 0000:02:02.1 -l 4,5,13,6,14 -n 6 -- --buffer-sz 64,128,256,512,1024,2048 --optype cipher-then-auth --ptest throughput --auth-key-sz 64 --cipher-key-sz 16 --devtype crypto_qat --cipher-iv-sz 16 --auth-op generate --burst-sz 32 --total-ops 30000000 --silent --digest-sz 32 --auth-algo sha2-256-hmac --cipher-algo aes-cbc --cipher-op encrypt`
Command line (AES-GCM-128)	`./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perf --socket-mem 2048,0 -w 0000:02:01.0 -w 0000:02:01.1 -w 0000:02:02.0 -w 0000:02:02.1 -l 4,5,13,6,14 -n 6 -- --aead-key-sz 16 --buffer-sz 64,128,256,512,1024,2048 --optype aead --ptest throughput --aead-aad-sz 16 --devtype crypto_qat --aead-op encrypt --burst-sz 32 --total-ops 30000000 --silent --digest-sz 16 --aead-algo aes-gcm --aead-iv-sz 12`
Notes	Use multi-cores configuration for testing is aim to reach maximum of QAT capability

Test Result:

Buffer Size(Bytes)	AES-CBC-128/SHA1-HMAC (Gbps)	AES-CBC-128/SHA2-256-HMAC(Gbps)	AES-GCM-128 (Gbps)
64	3.71	3.70	3.18
128	7.37	7.34	6.33
256	14.01	14.30	12.48
512	27.20	26.92	23.70
1024	45.34	45.87	38.61
2048	51.40	52.38	50.00



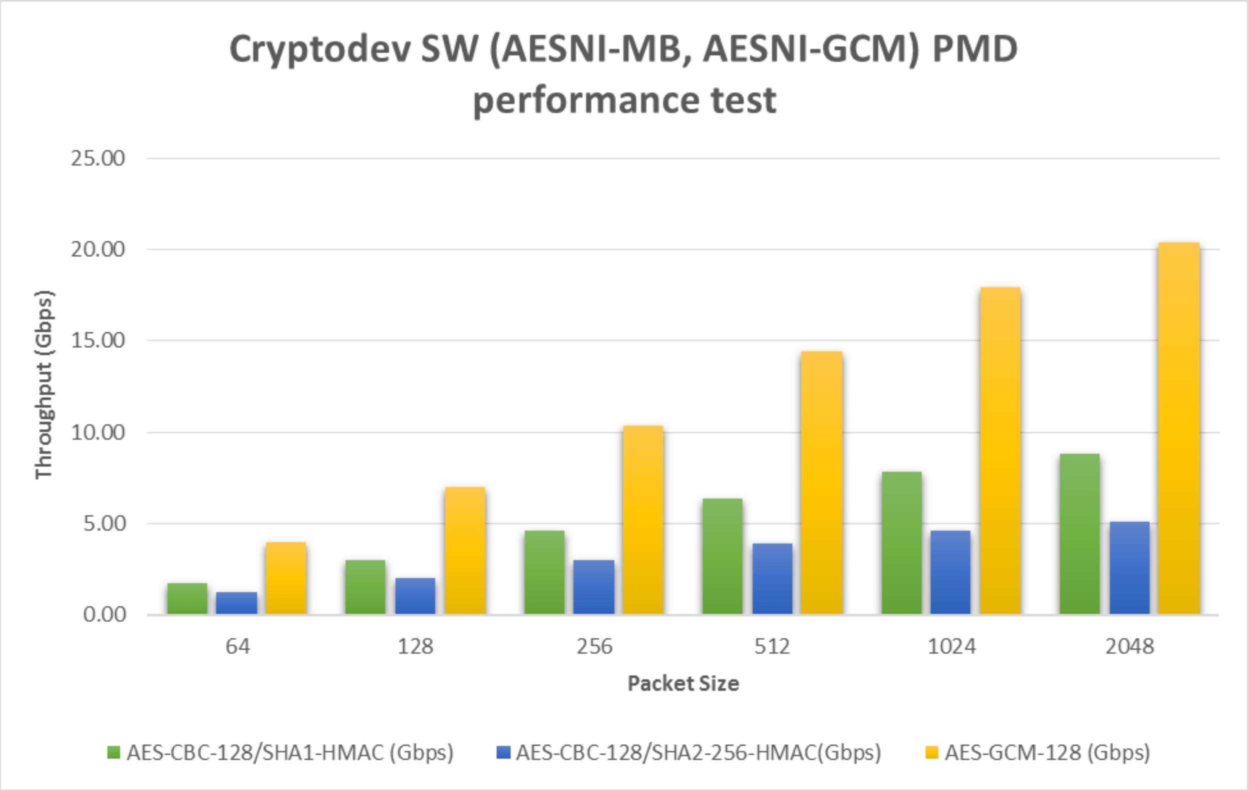
Test Case 4 – Cryptodev SW (AESNI-MB, AESNI-GCM) PMD performance test

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-perf --socket-mem 2048,0 --vdev crypto_aesni_mb_pmd_1 -l 4,5 -n 4 -- --buffer-sz 64,128,256,512,1024,2048 --optype cipher-then-auth --ptest throughput --auth-key-sz 64 --cipher-key-sz 16 --devtype crypto_aesni_mb --cipher-iv-sz 16 --auth-op generate --burst-sz 32 --total-ops 10000000 --silent --digest-sz 12 --auth-algo sha1-hmac --cipher-algo aes-cbc --cipher-op encrypt`
Command line (AES-CBC-128/SHA2-256-HMAC)	`./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perf --socket-mem 2048,0 --vdev crypto_aesni_mb_pmd_1 -l 4,5 -n 4 -- --buffer-sz 64,128,256,512,1024,2048 --optype cipher-then-auth --ptest throughput --auth-key-sz 64 --cipher-key-sz 16 --devtype crypto_aesni_mb --cipher-iv-sz 16 --auth-op generate --burst-sz 32 --total-ops 10000000 --silent --digest-sz 16 --auth-algo sha2-256-hmac --cipher-algo aes-cbc --cipher-op encrypt`
Command line (AES-GCM-128)	`./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perf --socket-mem 2048,0 --vdev crypto_aesni_gcm_pmd_1 -l 4,5 -n 4 -- --aead-key-sz 16 --buffer-sz 64,128,256,512,1024,2048 --optype aead --ptest throughput --aead-aad-sz 16 --devtype crypto_aesni_gcm --aead-op encrypt --burst-sz 32 --total-ops 10000000 --silent --digest-sz 16 --aead-algo aes-gcm --aead-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.

Test Result:

Buffer Size(Bytes)	AES-CBC-128/SHA1-HMAC (Gbps)	AES-CBC-128/SHA2-256-HMAC(Gbps)	AES-GCM-128 (Gbps)
64	1.77	1.22	3.97
128	3.01	2.03	6.87
256	4.64	2.99	10.32
512	6.37	3.90	14.34
1024	7.83	4.63	17.84
2048	8.84	5.07	20.27



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	SE5C610.86B.01.01.0016.033120161139
Linux kernel version	4.4.0-98-generic
GCC version	gcc (Ubuntu 5.4.0-6ubuntu1~16.04.5)
DPDK version	18.02

Boot and BIOS settings

Item	Description
Boot settings	`intel_iommu=on iommu=pt intel_pstate=disable isolcpus=8-15 nohz_full=8-15 rcu_nocbs=8-15 hugepagesz=1G hugepages=4 default_hugepagesz=1G`
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=y`
	`CONFIG_RTE_LIBRTE_PMD_AESNI_MB=y`
	`CONFIG_RTE_LIBRTE_PMD_AESNI_GCM=y`

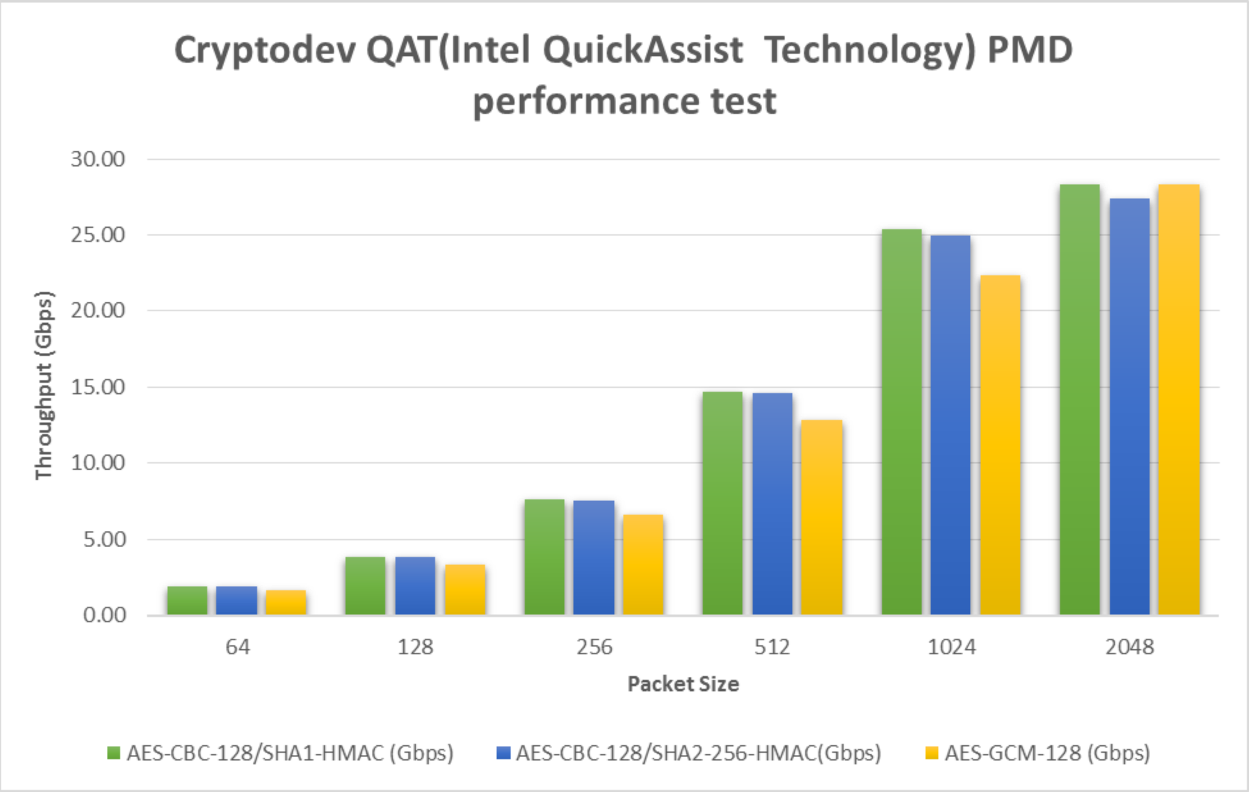
Test Case 5 – Cryptodev QAT(Intel QuickAssist Technology) PMD performance test

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 (AES-CBC-	`./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perf --socket-mem 2048,0 -w 0000:01:02.0 -w 0000:01:02.1 -w 0000:01:02.2 -w 0000:01:02.3 -l 4,5,6,7,8 -n 2  -- --buffer-sz 64,128,256,512,1024,2048 --optype cipher-then-auth --ptest throughput --auth-key-sz 64 --cipher-`

128/SHA1-HMAC)	`key-sz 16 --devtype crypto_qat --cipher-iv-sz 16 --auth-op generate --burst-sz 32 --total-ops 30000000 --silent  --digest-sz 20 --auth-algo sha1-hmac --cipher-algo aes-cbc --cipher-op encrypt`
Command line (AES-CBC-128/SHA2-256-HMAC)	`./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perf --socket-mem 2048,0 -w 0000:01:02.0 -w 0000:01:02.1 -w 0000:01:02.2 -w 0000:01:02.3 -l 4,5,6,7,8 -n 2 -- --buffer-sz 64,128,256,512,1024,2048 --optype cipher-then-auth --ptest throughput --auth-key-sz 64 --cipher-key-sz 16 --devtype crypto_qat --cipher-iv-sz 16 --auth-op generate --burst-sz 32 --total-ops 30000000 --silent --digest-sz 32 --auth-algo sha2-256-hmac --cipher-algo aes-cbc --cipher-op encrypt`
Command line (AES-GCM-128)	`./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perf --socket-mem 2048,0 -w 0000:01:02.0 -w 0000:01:02.1 -w 0000:01:02.2 -w 0000:01:02.3 -l 4,5,6,7,8 -n 2 -- --aead-key-sz 16 --buffer-sz 64,128,256,512,1024,2048 --optype aead --ptest throughput --aead-aad-sz 16 --devtype crypto_qat --aead-op encrypt --burst-sz 32 --total-ops 30000000 --silent --digest-sz 16 --aead-algo aes-gcm --aead-iv-sz 12`
Notes	Use multi-cores configuration for testing is aim to reach maximum of QAT capability

Test Result:

Buffer Size(Bytes)	AES-CBC-128/SHA1-HMAC (Gbps)	AES-CBC-128/SHA2-256-HMAC(Gbps)	AES-GCM-128 (Gbps)
64	1.94	1.93	1.66
128	3.86	3.84	3.32
256	7.62	7.57	6.58
512	14.68	14.56	12.80
1024	25.35	24.94	22.35
2048	28.32	27.48	28.32

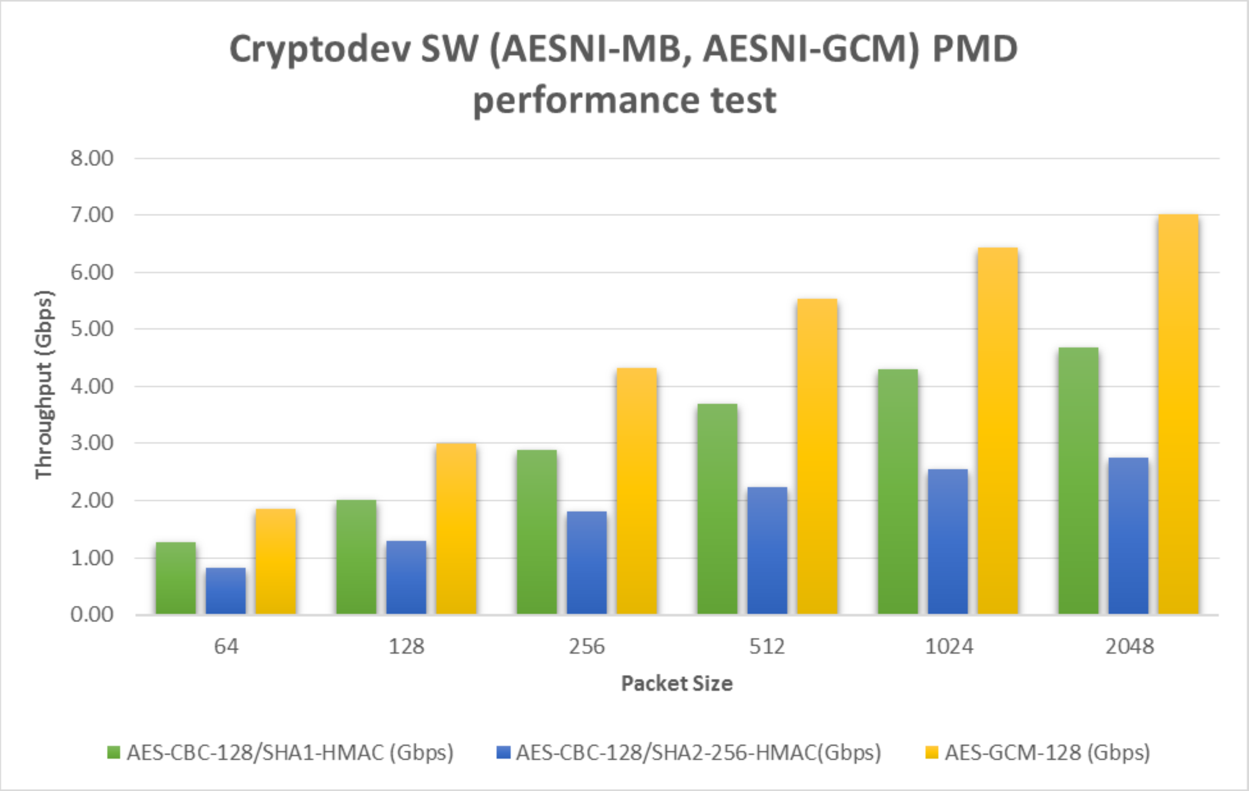


Test Case 6 – Cryptodev SW (AESNI-MB, AESNI-GCM) PMD performance test

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-perf --socket-mem 2048,0 --vdev crypto_aesni_mb_pmd_1 -l 4,5 -n 2 -- --buffer-sz 64,128,256,512,1024,2048 --optype cipher-then-auth --ptest throughput --auth-key-sz 64 --cipher-key-sz 16 --devtype crypto_aesni_mb --cipher-iv-sz 16 --auth-op generate --burst-sz 32 --total-ops 10000000 --silent --digest-sz 12 --auth-algo sha1-hmac --cipher-algo aes-cbc --cipher-op encrypt`
Command line (AES-CBC-128/SHA2-256-HMAC)	`./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perf --socket-mem 2048,0 --vdev crypto_aesni_mb_pmd_1 -l 4,5 -n 2 -- --buffer-sz 64,128,256,512,1024,2048 --optype cipher-then-auth --ptest throughput --auth-key-sz 64 --cipher-key-sz 16 --devtype crypto_aesni_mb --cipher-iv-sz 16 --auth-op generate --burst-sz 32 --total-ops 10000000 --silent --digest-sz 16 --auth-algo sha2-256-hmac --cipher-algo aes-cbc --cipher-op encrypt`
Command line (AES-GCM-128)	`./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-crypto-perf --socket-mem 2048,0 --vdev crypto_aesni_gcm_pmd_1 -l 4,5 -n 2 -- --aead-key-sz 16 --buffer-sz 64,128,256,512,1024,2048 --optype aead --ptest throughput --aead-aad-sz 16 --devtype crypto_aesni_gcm --aead-op encrypt --burst-sz 32 --total-ops 10000000 --silent --digest-sz 16 --aead-algo aes-gcm --aead-iv-sz 12`
Notes	The SW PMD performance is linear scaling out with core numbers. The scale factor is around 1.

Test Result:

Buffer Size(Bytes)	AES-CBC-128/SHA1-HMAC (Gbps)	AES-CBC-128/SHA2-256-HMAC(Gbps)	AES-GCM-128 (Gbps)
64	1.27	0.83	1.85
128	2.02	1.30	3.00
256	2.89	1.80	4.33
512	3.70	2.24	5.53
1024	4.30	2.55	6.42
2048	4.68	2.75	7.02


Cryptodev SW (AESNI-MB, AESNI-GCM) PMD performance test
Throughput (Gbps)
8.00
7.00
6.00
5.00
4.00
3.00
2.00
1.00
0.00
64
128
256
512
1024
2048
Packet Size
🟩 AES-CBC-128/SHA1-HMAC (Gbps)
🟦 AES-CBC-128/SHA2-256-HMAC(Gbps)
🟨 AES-GCM-128 (Gbps)

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.

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/**

§