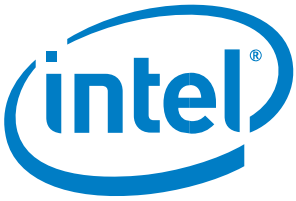


# DPDK Intel Cryptodev and IPSec Performance Report Release 19.11

**Test Date:** December 2nd 2019

**Author**: Intel DPDK Validation team

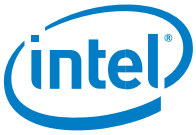


## *Revision History*

| Date | Revision | Comment |
|---|---|---|
| December 2nd, 2019 | 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.

# Crypto 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.

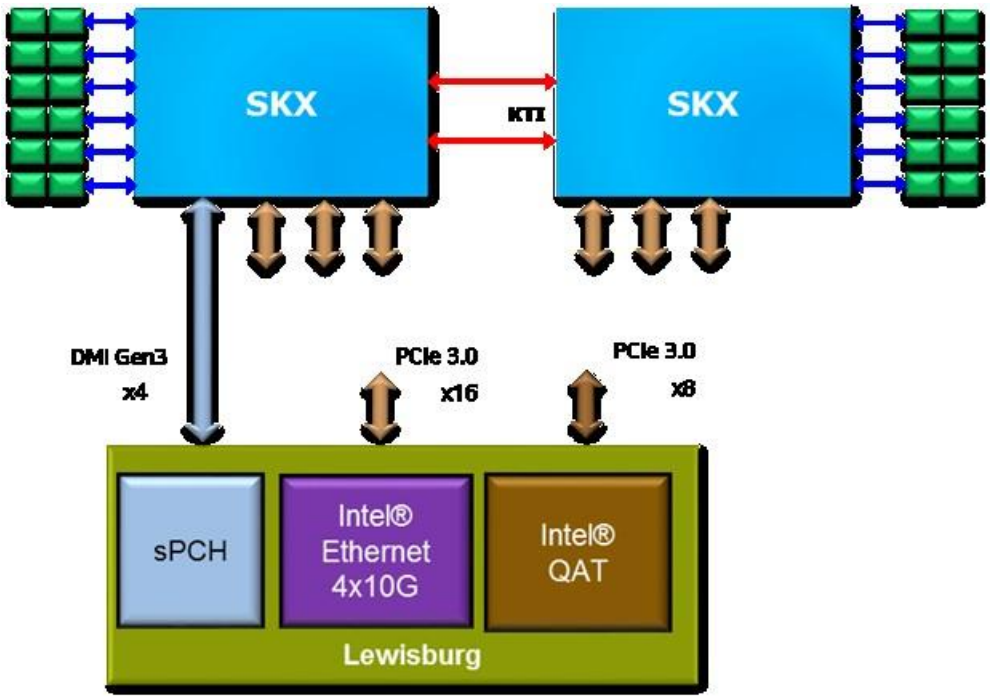



Figure1. DPDK cryptodev performance test setup

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

## Hardware & Software Ingredients

| Item | Description |
|---|---|
| Server Platform | PURLEY |
| Chipset | Intel® C620 Series Chipset |
| CPU | Intel(R) Xeon(R) Platinum 8180 CPU @ 2.50GHz<br>https://ark.intel.com/products/120496/Intel-Xeon-Platinum-8180-Processor38_5M-Cache-2_50-GHz<br>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 | Ubuntu18.04 |
| BIOS | SE5C620.86B.00.01.0009.101920170742 |
| Microcode version | 0x200005e |
| Linux kernel version | 4.15.0-55-generic |
| GCC version | 7.4.0 |
| DPDK version | 19.11 |

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><br>Package C-state Disabled<br>Hardware P-state Disabled<br>Enhanced Intel® Speedstep® Tech Disabled Intel®Turbo Boost Technology Disabled |
| DPDK Settings | Build Options: config/common_base<br>`CONFIG_RTE_LIBRTE_PMD_QAT_SYM=y`<br>`CONFIG_RTE_LIBRTE_PMD_AESNI_MB=y`<br>`CONFIG_RTE_LIBRTE_PMD_AESNI_GCM=y` |

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

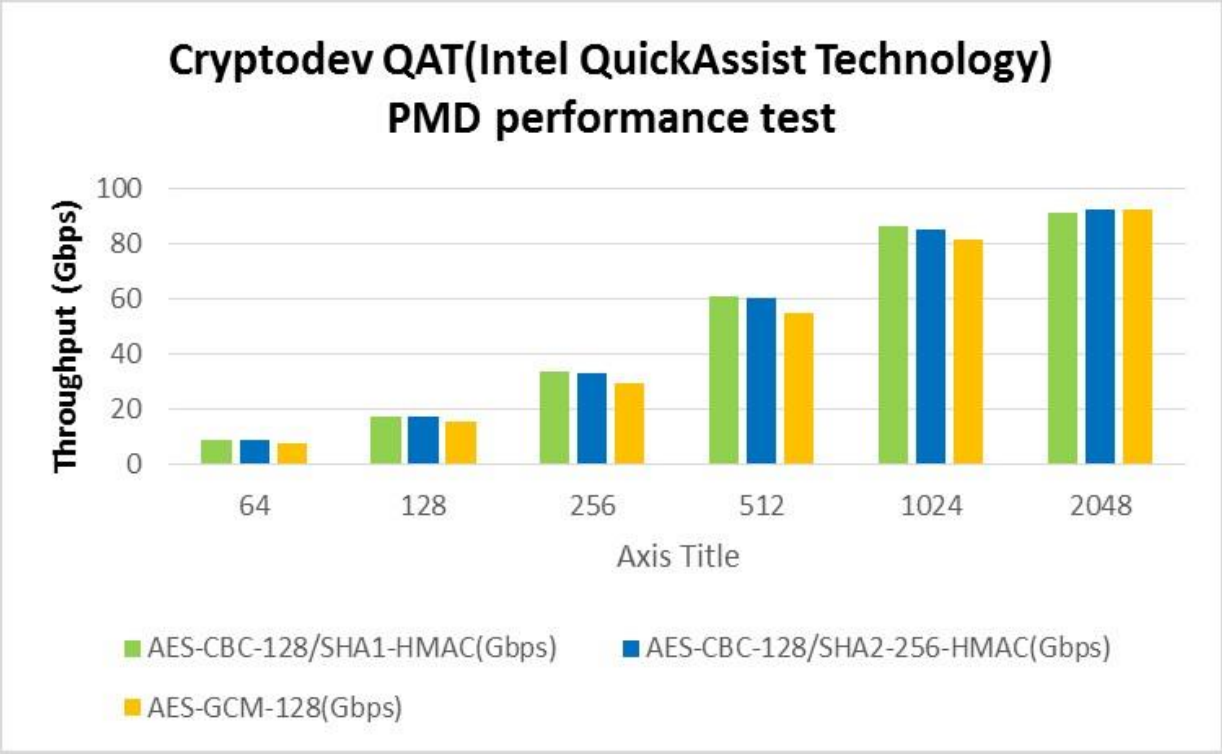
| Item | Description |
|---|---|
| Test Case | Cryptodev performance for AES-CBC-128/SHA1-HMAC, AES-GCM-128, AES-CBC128/SHA2-256-HMAC with Intel QuickAssist Technology |
| Cores | 3C6T |
| QAT | Integrated Intel QuickAssist Technology , PCI-e x16 Mode |

| | |
|---|---|
| Command line (AES-CBC128/SHA1-HMAC) | ./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-cryptoperf --socket-mem 2048,0 --legacy-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 0000:1c:01.2 -w 0000:1e:01.2 -w 0000:1a:01.3 -w 0000:1c:01.3 -w 0000:1e:01.3 -w 0000:1a:01.4 -w 0000:1c:01.4 -w 0000:1e:01.4 -w 0000:1a:01.5 -w 0000:1c: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=0000:1e:01.0_qat_sym,mode=round-robin --vdev=crypto_scheduler_pmd_2,slave=0000:1a:01.1_qat_sym,slave=0000:1c:01.1_qat_sym,slave=0000:1e:01.1_qat_sym,mode=round-robin --vdev=crypto_scheduler_pmd_3,slave=0000:1a:01.2_qat_sym,slave=0000:1c:01.2_qat_sym,slave=0000:1e:01.2_qat_sym,mode=round-robin --vdev=crypto_scheduler_pmd_4,slave=0000:1a: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 -l 9,10,66,11,67,12,68 -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-CBC128/SHA2-256HMAC) | ./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-cryptoperf --socket-mem 2048,0 --legacy-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 0000:1c:01.2 -w 0000:1e:01.2 -w 0000:1a:01.3 -w 0000:1c:01.3 -w 0000:1e:01.3 -w 0000:1a:01.4 -w 0000:1c:01.4 -w 0000:1e:01.4 -w 0000:1a:01.5 -w 0000:1c: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=0000:1e:01.0_qat_sym,mode=round-robin --vdev=crypto_scheduler_pmd_2,slave=0000:1a:01.1_qat_sym,slave=0000:1c:01.1_qat_sym,slave=0000:1e:01.1_qat_sym,mode=round-robin --vdev=crypto_scheduler_pmd_3,slave=0000:1a:01.2_qat_sym,slave=0000:1c:01.2_qat_sym,slave=0000:1e:01.2_qat_sym,mode=round-robin --vdev=crypto_scheduler_pmd_4,slave=0000:1a: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 -l 9,10,66,11,67,12,68 -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-cryptoperf --socket-mem 2048,0 --legacy-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 0000:1c:01.2 -w 0000:1e:01.2 -w 0000:1a:01.3 -w 0000:1c:01.3 -w 0000:1e:01.3 -w 0000:1a:01.4 -w 0000:1c:01.4 -w 0000:1e:01.4 -w 0000:1a:01.5 -w 0000:1c: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=0000:1e:01.0_qat_sym,mode=round-robin --vdev=crypto_scheduler_pmd_2,slave=0000:1a:01.1_qat_sym,slave=0000:1c:01.1_qat_sym,slave=0000:1e:01.1_qat_sym,mode=round-robin --vdev=crypto_scheduler_pmd_3,slave=0000:1a:01.2_qat_sym,slave=0000:1c:01.2_qat_sym,slave=0000:1e:01.2_qat_sym,mode=round-robin --vdev=crypto_scheduler_pmd_4,slave=0000:1a: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 -l 9,10,66,11,67,12,68 -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 | 8.89 | 8.82 | 7.71 |
| 128 | 17.44 | 17.27 | 15.25 |
| 256 | 33.48 | 33.13 | 29.67 |
| 512 | 60.67 | 60.31 | 54.56 |
| 1024 | 86.68 | 85.24 | 81.76 |
| 2048 | 91.26 | 92.71 | 92.77 |

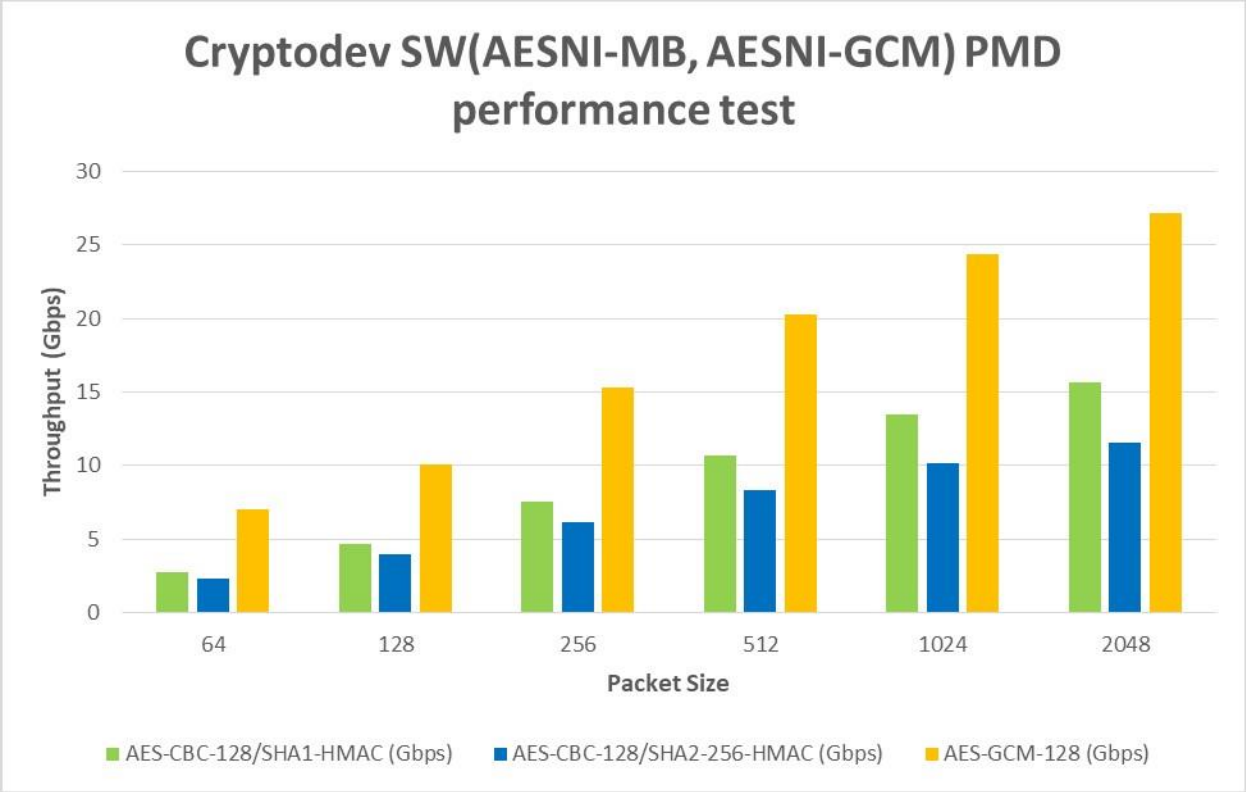


# Test Case 2 – Cryptodev SW (AESNI-MB, AESNI-GCM) PMD performance test

| Item | Description |
|---|---|
| Test Case | Cryptodev performance for AES-CBC-128/SHA1-HMAC, AES-GCM-128, AES-CBC128/SHA2-256-HMAC, KASUMI-F8/KASUMI-F9, SNOW3G-UEA2/SNOW3G-UIA2, ZUC-EEA3/ZUC-EIA3 |
| Cores | 1C1T |
| QAT | Not use |
| Command line (AES-CBC128/SHA1-HMAC) | `./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-cryptoperf --socket-mem 2048,0 --legacy-mem --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-CBC128/SHA2-256HMAC) | `./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-cryptoperf --socket-mem 2048,0 --legacy-mem --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-cryptoperf --socket-mem 2048,0 --legacy-mem --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.<br>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 | 2.97 | 2.44 | 6.79 |
| 128 | 5.08 | 4.11 | 9.69 |
| 256 | 8.01 | 6.26 | 14.75 |
| 512 | 11.10 | 8.45 | 19.81 |
| 1024 | 13.81 | 10.29 | 24.05 |
| 2048 | 15.78 | 11.55 | 26.91 |


Cryptodev SW(AESNI-MB, AESNI-GCM) PMD performance test
Throughput (Gbps)
30
25
20
15
10
5
0
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)

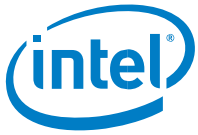
# Intel® Xeon® Processor D-1553N (12M Cache, 2.30 GHz)

## Hardware & Software Ingredients

| Item | Description |
|---|---|
| Server Platform | GRANGEVILLE |
| CPU | Intel® Xeon® Processor D-1553N (12M Cache, 2.30 GHz)<br>https://ark.intel.com/products/123002/Intel-Xeon-Processor-D-1553N-12MCache-2_30-GHz<br>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 | 0xe00000f |
| Linux kernel version | 4.15.0-72-generic |
| GCC version | 5.4.0 20160609 |
| DPDK version | 19.11 |

Boot and BIOS settings

| Item | Description |
|---|---|
| Boot settings | `intel_iommu=on iommu=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` |
| BIOS | Boot performance mode <Max Performance><br>CPU C state Disabled<br>Energy efficient P-state Disabled<br>Turbo Mode Disabled |
| DPDK Settings | Build Options: config/common_base<br>`CONFIG_RTE_LIBRTE_PMD_QAT_SYM=y`<br>`CONFIG_RTE_LIBRTE_PMD_AESNI_MB=y`<br>`CONFIG_RTE_LIBRTE_PMD_AESNI_GCM=y` |

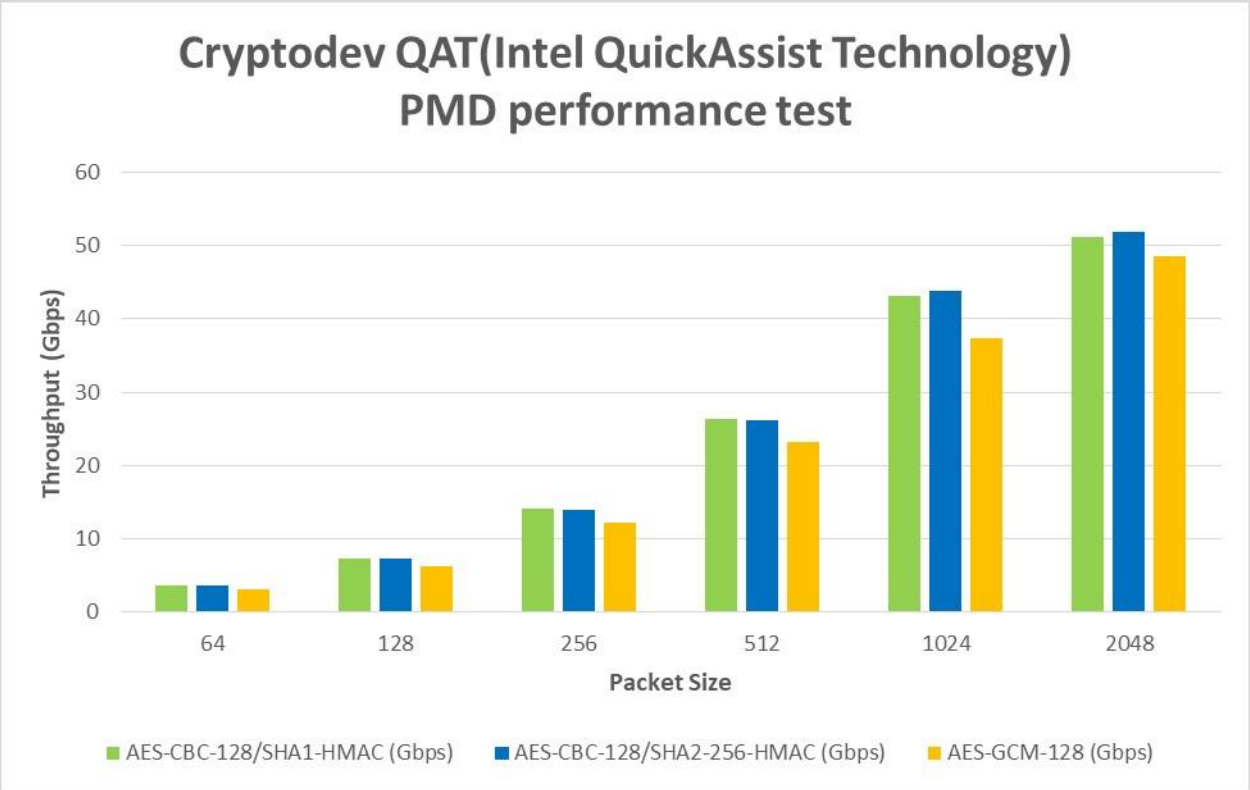


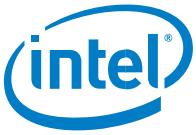
# Test Case 3 – Cryptodev QAT(Intel QuickAssist Technology) PMD performance test

| Item | Description |
|---|---|
| Test Case | Cryptodev performance for AES-CBC-128/SHA1-HMAC, AES-GCM-128, AES-CBC128/SHA2-256-HMAC by Intel QuickAssist Technology |
| Cores | 2C4T |
| QAT | Integrated Intel QuickAssist Technology |
| Command line (AES-CBC128/SHA1-HMAC) | `./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-cryptoperf --socket-mem 2048,0 --legacy-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 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_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-CBC128/SHA2-256HMAC) | `./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-cryptoperf --socket-mem 2048,0 --legacy-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 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_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-cryptoperf --socket-mem 2048,0 --legacy-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 4 -- --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-ivsz 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 | 3.47 | 3.46 | 3.17 |
| 128 | 6.84 | 6.81 | 6.29 |
| 256 | 13.20 | 13.12 | 12.27 |
| 512 | 25.05 | 24.81 | 23.02 |
| 1024 | 41.92 | 42.27 | 37.08 |
| 2048 | 50.60 | 51.45 | 48.02 |


Cryptodev QAT(Intel QuickAssist Technology)
PMD performance test
Throughput (Gbps)
60
50
40
30
20
10
0
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)

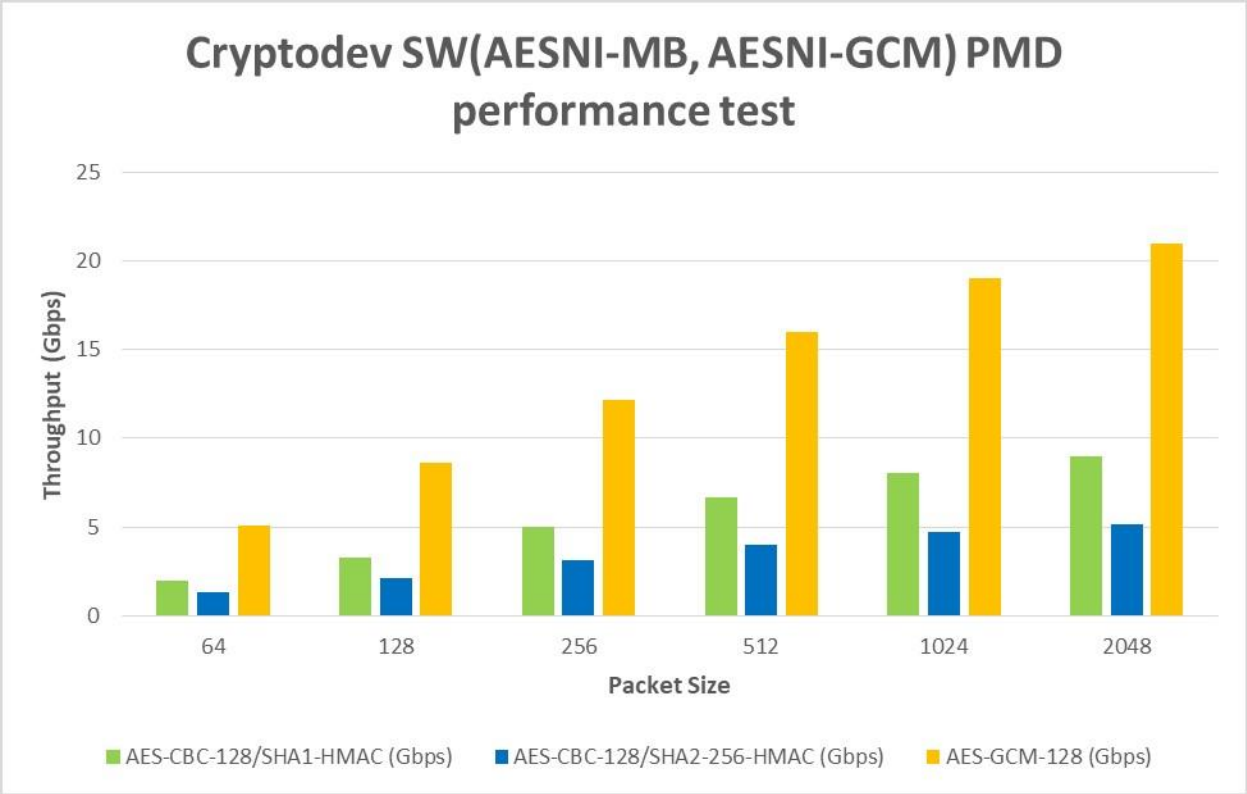


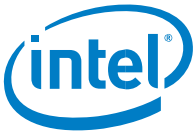
# Test Case 4 – Cryptodev SW (AESNI-MB, AESNI-GCM) PMD performance test

| Item | Description |
|---|---|
| Test Case | Cryptodev performance for AES-CBC-128/SHA1-HMAC, AES-GCM-128, AES-CBC128/SHA2-256-HMAC |
| Cores | 1C1T |
| QAT | Not use |
| Command line (AES-CBC128/SHA1-HMAC) | `./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-cryptoperf --socket-mem 2048,0 --legacy-mem --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-CBC128/SHA2-256HMAC) | `./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-cryptoperf --socket-mem 2048,0 --legacy-mem --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-cryptoperf --socket-mem 2048,0 --legacy-mem --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.<br>The scale factor is around 1. If the hyper-threading is enabled, extra ~20%-50% performance will be achieved per hyper-thread.<br>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 | 2.22 | 1.44 | 4.96 |
| 128 | 3.64 | 2.29 | 8.51 |
| 256 | 5.37 | 3.26 | 12.03 |
| 512 | 7.05 | 4.13 | 15.83 |
| 1024 | 8.32 | 4.78 | 18.80 |
| 2048 | 9.17 | 5.17 | 20.82 |


Cryptodev SW(AESNI-MB, AESNI-GCM) PMD performance test
Throughput (Gbps)
25
20
15
10
5
0
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 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)<br>https://ark.intel.com/products/series/97941/Intel-Atom-Processor-C-Series<br>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 | 0x2e |
| Linux kernel version | 4.15.0-72-generic |
| GCC version | 5.4.0 20160609 |
| DPDK version | 19.11 |

Boot and BIOS settings

| Item | Description |
|---|---|
| Boot settings | `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` |
| BIOS | Energy Performance Bias <Performance><br>CPU C state Disabled<br>Turbo Disabled |
| DPDK Settings | Build Options: config/common_base<br>`CONFIG_RTE_LIBRTE_PMD_QAT_SYM=y`<br>`CONFIG_RTE_LIBRTE_PMD_AESNI_MB=y`<br>`CONFIG_RTE_LIBRTE_PMD_AESNI_GCM=y` |

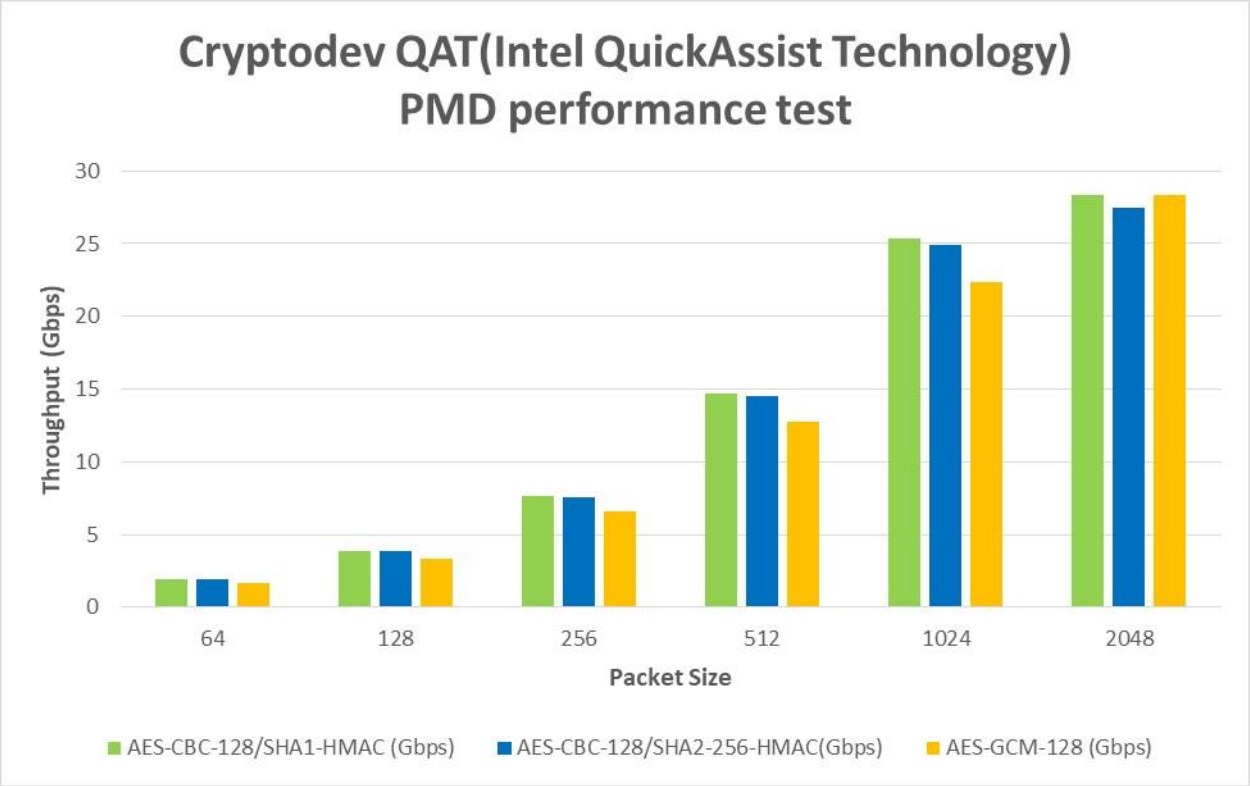
## Test Case 5 – Cryptodev QAT(Intel QuickAssist Technology) PMD performance test

| Item | Description |
|---|---|
| Test Case | Cryptodev performance for AES-CBC-128/SHA1-HMAC, AES-GCM-128, AES-CBC128/SHA2-256-HMAC by Intel QuickAssist Technology |
| Cores | 4C4T |

| | |
|---|---|
| QAT | Integrated Intel QuickAssist Technology |
| Command line (AES-CBC128/SHA1-HMAC) | `./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-cryptoperf --socket-mem 2048,0 --legacy-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 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 20 --auth-algo sha1-hmac --cipher-algo aes-cbc --cipher-op encrypt` |
| Command line (AES-CBC128/SHA2-256HMAC) | `./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-cryptoperf --socket-mem 2048,0 --legacy-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 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-cryptoperf --socket-mem 2048,0 --legacy-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 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-ivsz 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 | 14.55 | 12.80 |
| 1024 | 25.34 | 24.90 | 22.34 |
| 2048 | 28.33 | 27.44 | 28.29 |

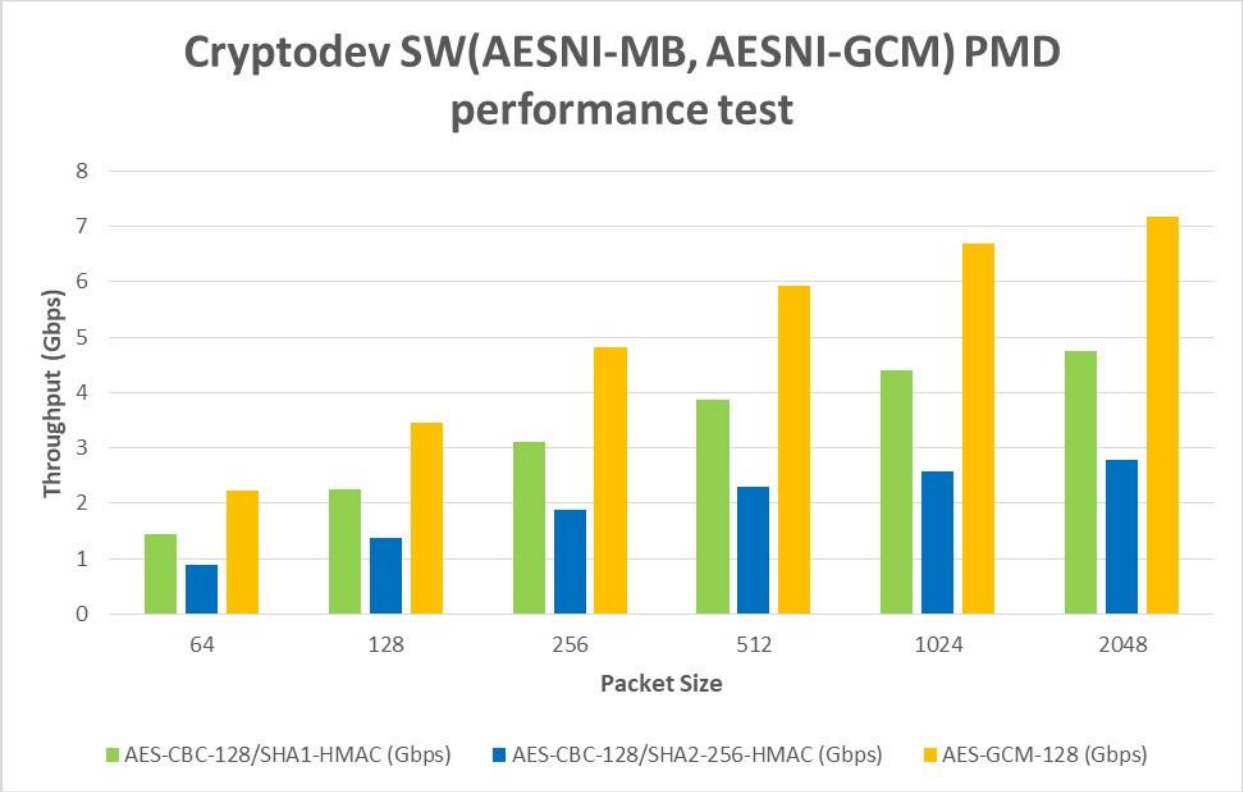

Cryptodev QAT(Intel QuickAssist Technology)
PMD performance test
Throughput (Gbps)
30
25
20
15
10
5
0
64
128
256
512
1024
2048
Packet Size
AES-CBC-128/SHA1-HMAC (Gbps)
AES-CBC-128/SHA2-256-HMAC(Gbps)
AES-GCM-128 (Gbps)

# 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-CBC128/SHA2-256-HMAC |
| Cores | 1C1T |
| QAT | Not use |
| Command line (AES-CBC128/SHA1-HMAC) | `./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-cryptoperf --socket-mem 2048,0 --legacy-mem --vdev crypto_aesni_mb_pmd_1 -l 6,7 -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-CBC128/SHA2-256HMAC) | `./x86_64-native-linuxapp-gcc/build/app/test-crypto-perf/dpdk-test-cryptoperf --socket-mem 2048,0 --legacy-mem --vdev crypto_aesni_mb_pmd_1 -l 6,7 -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-cryptoperf --socket-mem 2048,0 --legacy-mem --vdev crypto_aesni_gcm_pmd_1 -l 6,7 -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 | 1.45 | 0.90 | 2.20 |
| 128 | 2.28 | 1.38 | 3.41 |
| 256 | 3.12 | 1.88 | 4.75 |
| 512 | 3.88 | 2.30 | 5.89 |
| 1024 | 4.41 | 2.59 | 6.67 |
| 2048 | 4.75 | 2.77 | 7.16 |


Cryptodev SW(AESNI-MB, AESNI-GCM) PMD performance test
Throughput (Gbps)
0
1
2
3
4
5
6
7
8
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)

# IPSec 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 ipsec-secgw Test Case**: Documentation may be found at https://doc.dpdk.org/guides/sample_app_ug/ipsec_secgw.html.

The application demonstrates the use of IPSec library in the DPDK to implement an IPSec gateway. The gateway could establish an IPSec tunnel between two nodes to provide a security transport layer.

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.

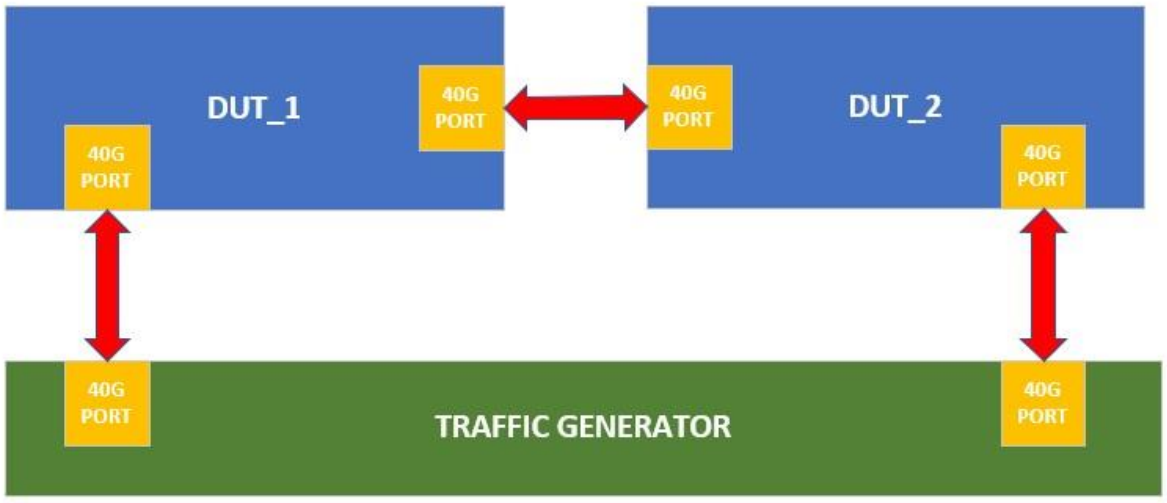



Figure1. DPDK IPSec performance test setup

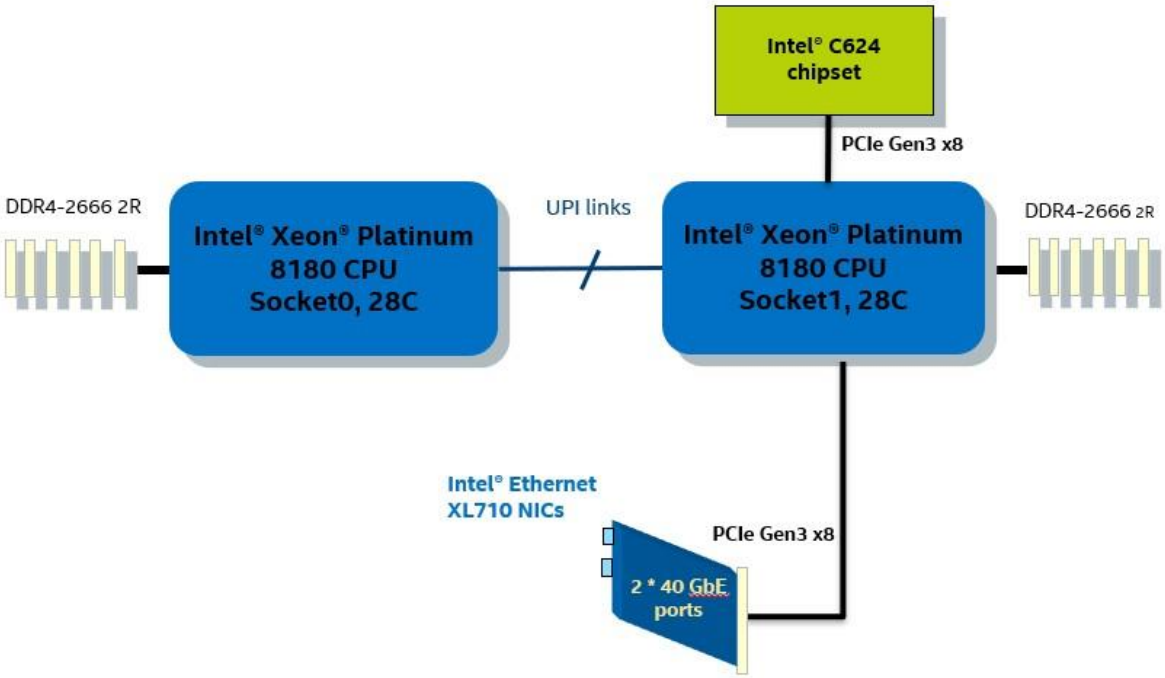



Figure2. Device Under Test Setup (DUT)

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

## Hardware & Software Ingredients

| Item | Description |
|---|---|
| Server Platform | Intel® Server Board S2600WFT Intel® Server Board S2600WFT Family |
| Chipset | Intel® C620 Series Chipset |
| CPU | Intel(R) Xeon(R) Platinum 8180 CPU @ 2.50GHz<br>https://ark.intel.com/products/120496/Intel-Xeon-Platinum-8180-Processor38_5M-Cache-2_50-GHz<br>Number of cores 28/socket, Number of threads 56/socket |
| Memory | Total 98304 MBs over 12 channels @ 2133 MHz |
| PCIe | 3 x PCIe Gen3 x8 slots |
| NIC | 40GbE XL710 |
| QAT | PCI-e x8 Gen3 mode |

| | |
|---|---|
| Operating System | Ubuntu19.04 |
| BIOS | SE5C620.86B.00.01.0009.101920170742 |
| Microcode version | 0x2000030 |
| Linux kernel version | 5.0.0-37-generic |
| GCC version | 8.3.0 |
| DPDK version | 19.11 |

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><br>CPU C-state Disabled<br>CPU P-state Disabled<br>Enhanced Intel® Speedstep® Tech Disabled<br>Turbo Boost Disabled |
| DPDK Settings | Build Options: config/common_base<br>`CONFIG_RTE_LIBRTE_PMD_QAT_SYM=y`<br>`CONFIG_RTE_LIBRTE_PMD_AESNI_MB=y`<br>`CONFIG_RTE_LIBRTE_PMD_AESNI_GCM=y` |

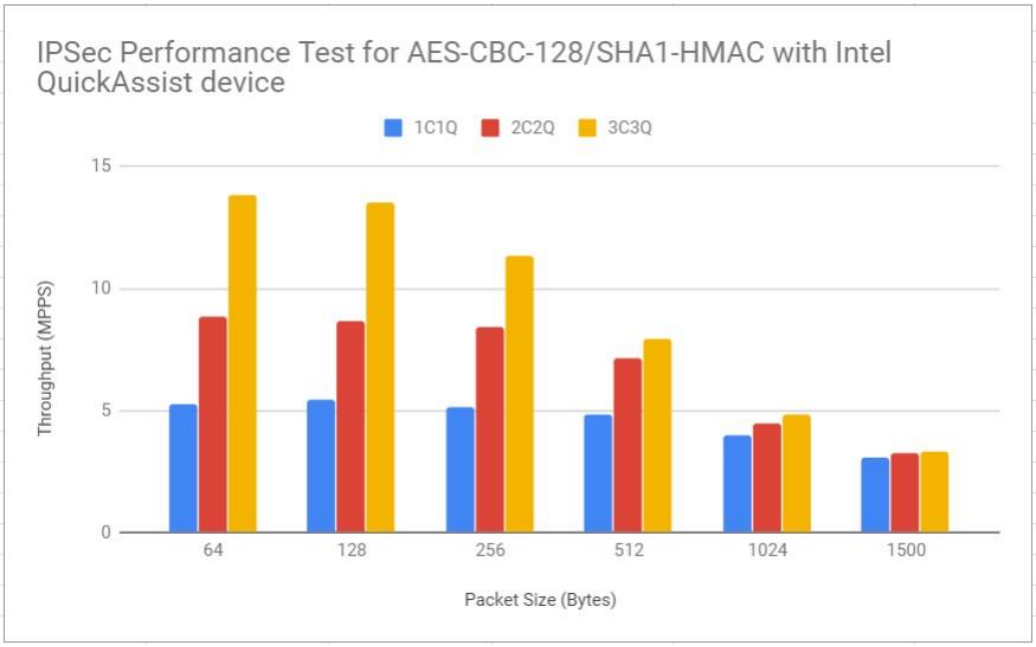
# Test Case 1 – IPSec Performance Test for AES-CBC128/SHA1-HMAC with Intel QuickAssist device

| Item | Description |
|---|---|
| Test Case | IPSec Performance Test for AES-CBC-128/SHA1-HMAC with Intel QuickAssist device |
| Cores (Cores/NIC and QAT Queue) | 1C1Q, 2C2Q, 3C3Q |
| QAT | Integrated Intel QuickAssist Technology , PCI-e x8 Mode |
| Command Line (AES-CBC128/SHA1-HMAC) | `./build/ipsec-secgw --lcores=40 -n 4 -w b7:00.0 -w b7:00.1 -w b1:01.0 -- p 0x3 -u 1 -P --config="(0,0,40),(1,0,40)" -f ./ipsec_test_cbc.cfg` |

| | |
|---|---|
| Config File (AES-CBC128/SHA1-HMAC) | #SP IPv4 rules<br>sp ipv4 out esp protect 1000 pri 5 dst 11.11.11.2/24 src 11.11.11.1/32 sport 0:65535 dport 0:65535<br>sp ipv4 out esp protect 1001 pri 5 dst 11.11.12.2/24 src 11.11.11.1/32 sport 0:65535 dport 0:65535<br>sp ipv4 out esp protect 1002 pri 5 dst 11.11.13.2/24 src 11.11.11.1/32 sport 0:65535 dport 0:65535<br>sp ipv4 out esp bypass pri 1 sport 0:65535 dport 0:65535<br><br>sp ipv4 in esp protect 1010 pri 5 dst 12.12.12.1/32 src 12.12.12.2/32 sport 0:65535 dport 0:65535<br>sp ipv4 in esp protect 1011 pri 5 dst 12.12.12.1/32 src 12.12.12.3/32 sport 0:65535 dport 0:65535<br>sp ipv4 in esp protect 1012 pri 5 dst 12.12.12.1/32 src 12.12.12.14/32 sport 0:65535 dport 0:65535<br>sp ipv4 in esp bypass pri 1 sport 0:65535 dport 0:65535<br>#SA rules<br>sa out 1000 cipher_algo aes-128-cbc cipher_key de:ad:be:ef:de:ad:be:ef:de:ad:be:ef:de:ad:be:ef auth_algo sha1-hmac auth_key de:ad:be:ef:de:ad:be:ef:de:ad:be:ef:de:ad:be:ef:de:ad:be:ef mode ipv4-tunnel src 12.12.12.1 dst 12.12.12.2 sa out 1001 cipher_algo aes-128-cbc cipher_key de:ad:be:ef:de:ad:be:ef:de:ad:be:ef:de:ad:be:ef auth_algo sha1-hmac auth_key de:ad:be:ef:de:ad:be:ef:de:ad:be:ef:de:ad:be:ef:de:ad:be:ef mode ipv4-tunnel src 12.12.12.1 dst 12.12.12.3 sa out 1002 cipher_algo aes-128-cbc cipher_key de:ad:be:ef:de:ad:be:ef:de:ad:be:ef:de:ad:be:ef auth_algo sha1-hmac auth_key de:ad:be:ef:de:ad:be:ef:de:ad:be:ef:de:ad:be:ef:de:ad:be:ef mode ipv4-tunnel src 12.12.12.1 dst 12.12.12.14<br><br>sa in 1010 cipher_algo aes-128-cbc cipher_key de:ad:be:ef:de:ad:be:ef:de:ad:be:ef:de:ad:be:ef auth_algo sha1-hmac auth_key de:ad:be:ef:de:ad:be:ef:de:ad:be:ef:de:ad:be:ef:de:ad:be:ef mode ipv4-tunnel src 12.12.12.2 dst 12.12.12.1 sa in 1011 cipher_algo aes-128-cbc cipher_key de:ad:be:ef:de:ad:be:ef:de:ad:be:ef:de:ad:be:ef auth_algo sha1-hmac auth_key de:ad:be:ef:de:ad:be:ef:de:ad:be:ef:de:ad:be:ef:de:ad:be:ef mode ipv4-tunnel src 12.12.12.3 dst 12.12.12.1 sa in 1012 cipher_algo aes-128-cbc cipher_key de:ad:be:ef:de:ad:be:ef:de:ad:be:ef:de:ad:be:ef auth_algo sha1-hmac auth_key de:ad:be:ef:de:ad:be:ef:de:ad:be:ef:de:ad:be:ef:de:ad:be:ef mode ipv4-tunnel src 12.12.12.14 dst 12.12.12.1<br><br>#Routing rules<br>rt ipv4 dst 12.12.12.2/24 port 0 rt<br>ipv4 dst 13.13.13.2/8 port 1<br><br>neigh port 0 1a:2b:3c:4d:5e:6f |

## Test Result (Mpackets/s):

| AES-CBC-128 | 64 | 128 | 256 | 512 | 1024 | 1500 |
|---|---|---|---|---|---|---|
| 1C1Q | 5.242 | 5.464 | 5.122 | 4.846 | 3.998 | 3.087 |
| 2C2Q | 8.823 | 8.648 | 8.415 | 7.146 | 4.463 | 3.234 |
| 3C3Q | 13.848 | 13.546 | 11.368 | 7.961 | 4.832 | 3.289 |



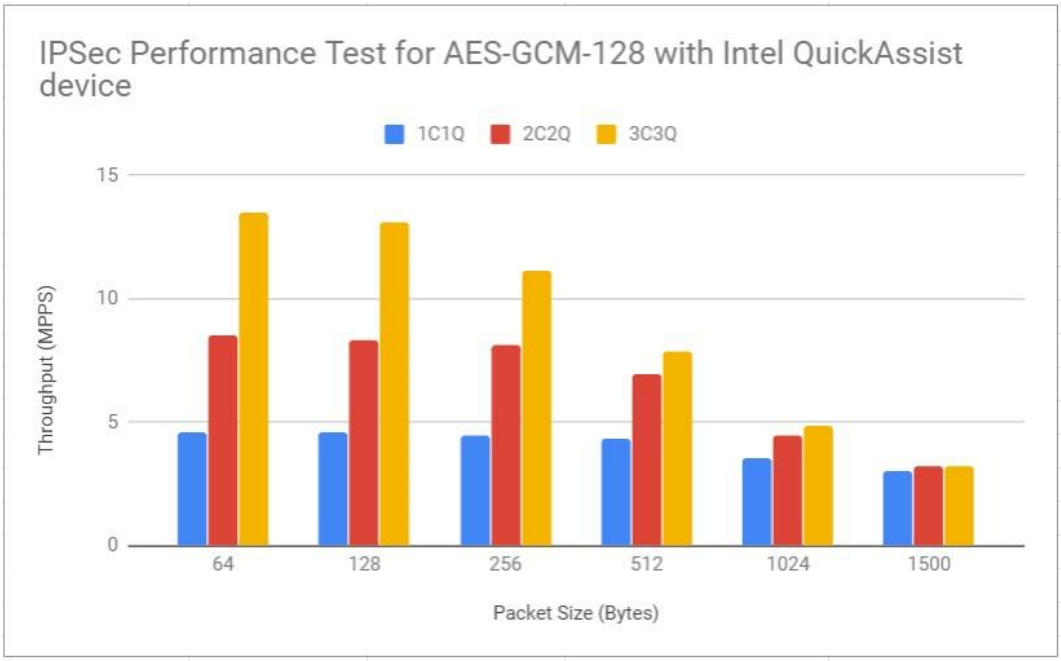

## Test Case 2 – IPSec Performance Test for AES-GCM-128 with Intel QuickAssist device

| Item | Description |
|---|---|
| Test Case | IPSec Performance Test for AES-GCM-128 with Intel QuickAssist device |
| Cores (Cores/NIC and QAT Queue) | 1C1Q, 2C2Q, 3C3Q |
| QAT (Cores/NIC and QAT Queue) | Integrated Intel QuickAssist Technology , PCI-e x8 Mode |
| Command Line (AES-GCM-128) | `./build/ipsec-secgw --lcores=40 -n 4 -w b7:00.0 -w b7:00.1 -w b1:01.0 -- p 0x3 -u 1 -P --config="(0,0,40),(1,0,40)" -f ./ipsec_test_gcm.cfg` |

| Config File (AES-GCM-128) | #SP IPv4 rules sp ipv4 out esp protect 1000 pri 5 dst 11.11.11.2/24 src 11.11.11.1/32 sport 0:65535 dport 0:65535 sp ipv4 out esp protect 1001 pri 5 dst 11.11.12.2/24 src 11.11.11.1/32 sport 0:65535 dport 0:65535 sp ipv4 out esp protect 1002 pri 5 dst 11.11.13.2/24 src 11.11.11.1/32 sport 0:65535 dport 0:65535 sp ipv4 out esp bypass pri 1 sport 0:65535 dport 0:65535<br>sp ipv4 in esp protect 1010 pri 5 dst 12.12.12.1/32 src 12.12.12.2/32 sport 0:65535 dport 0:65535 sp ipv4 in esp protect 1011 pri 5 dst 12.12.12.1/32 src 12.12.12.3/32 sport 0:65535 dport 0:65535 sp ipv4 in esp protect 1012 pri 5 dst 12.12.12.1/32 src 12.12.12.14/32 sport 0:65535 dport 0:65535 sp ipv4 in esp bypass pri 1 sport 0:65535 dport 0:65535<br>#SA rules sa out 1000 aead_algo aes-128-gcm aead_key<br>de:ad:be:ef:de:ad:be:ef:de:ad:be:ef:de:ad:be:ef mode ipv4tunnel src 12.12.12.1 dst 12.12.12.2 sa out 1001 aead_algo aes-128-gcm aead_key<br>de:ad:be:ef:de:ad:be:ef:de:ad:be:ef:de:ad:be:ef mode ipv4tunnel src 12.12.12.1 dst 12.12.12.3 sa out 1002 aead_algo aes-128-gcm aead_key<br>de:ad:be:ef:de:ad:be:ef:de:ad:be:ef:de:ad:be:ef mode ipv4tunnel src 12.12.12.1 dst 12.12.12.14<br>sa in 1010 aead_algo aes-128-gcm aead_key<br>de:ad:be:ef:de:ad:be:ef:de:ad:be:ef:de:ad:be:ef mode ipv4tunnel src 12.12.12.2 dst 12.12.12.1 sa in 1011 aead_algo aes-128-gcm aead_key<br>de:ad:be:ef:de:ad:be:ef:de:ad:be:ef:de:ad:be:ef mode ipv4tunnel src 12.12.12.3 dst 12.12.12.1 sa in 1012 aead_algo aes-128-gcm aead_key<br>de:ad:be:ef:de:ad:be:ef:de:ad:be:ef:de:ad:be:ef mode ipv4tunnel src 12.12.12.14 dst 12.12.12.1<br>#Routing rules rt ipv4 dst 12.12.12.2/24 port 0 rt ipv4 dst 13.13.13.2/8 port 1<br>neigh port 0 1a:2b:3c:4d:5e:6f |
|---|---|

## Test Result: (Mpackets / s)

| AES-GCM-128 | 64 | 128 | 256 | 512 | 1024 | 1500 |
|---|---|---|---|---|---|---|
| 1C1Q | 4.572 | 4.583 | 4.462 | 4.328 | 3.531 | 2.973 |
| 2C2Q | 8.524 | 8.323 | 8.124 | 6.958 | 4.479 | 3.223 |
| 3C3Q | 13.512 | 13.084 | 11.129 | 7.878 | 4.868 | 3.232 |

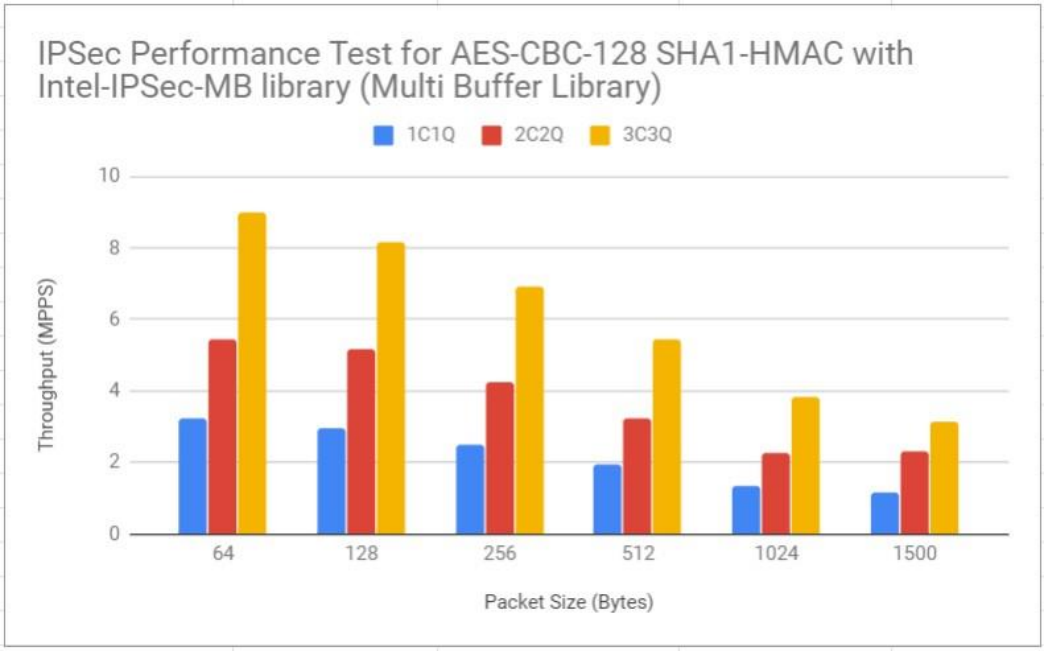

IPSec Performance Test for AES-GCM-128 with Intel QuickAssist device
1C1Q
2C2Q
3C3Q
15
10
5
0
Throughput (MPPS)
64
128
256
512
1024
1500
Packet Size (Bytes)

# Test Case 3 – IPSec Performance Test for AES-CBC128/SHA1-HMAC with Intel-IPSec-MB library

| Item | Description |
|---|---|
| Test Case | IPSec Performance Test for AES-CBC-128 SHA1-HMAC with Intel-IPSec-MB library (Multi Buffer Library) |
| IPSec-MB version | 0.52 |
| Cores | 1C1Q, 2C2Q, 3C3Q |
| QAT | Not Used |
| Command Line (AES-GCM-128) | `./build/ipsec-secgw --lcores=40 -n 4 -w b7:00.0 -w b7:00.1 -vdev="crypto_aesni_mb0,socket_id=1" -- -p 0x3 -u 1 -P -config="(0,0,40),(1,0,40)" -f ./ipsec_test_cbc.cfg` |

Test Result: (Mpackets /s)

| AES-CBC-128 | 64 | 128 | 256 | 512 | 1024 | 1500 |
|---|---|---|---|---|---|---|
| 1C1Q | 3.212 | 2.933 | 2.497 | 1.943 | 1.356 | 1.162 |
| 2C2Q | 5.451 | 5.146 | 4.238 | 3.223 | 2.247 | 2.312 |
| 3C3Q | 8.99 | 8.144 | 6.929 | 5.447 | 3.811 | 3.123 |

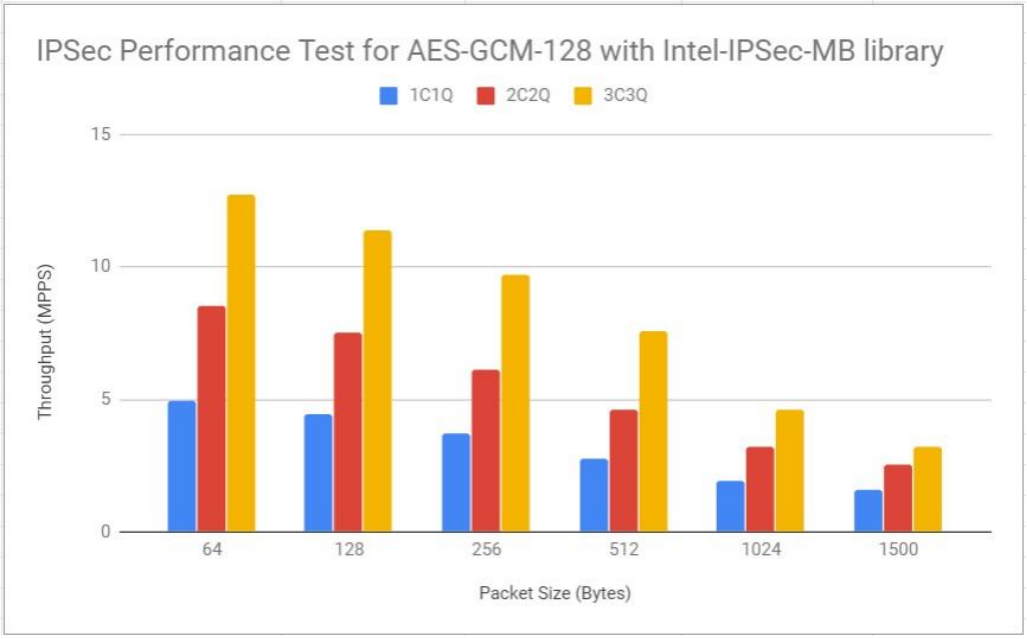


# Test Case 4 – IPSec Performance Test for AES-GCM-128 with Intel-IPSec-MB library

| Item | Description |
|---|---|
| Test Case | IPSec Performance Test for AES-GCM-128 with Intel-IPSec-MB library |
| IPSec-MB version | 0.52 |
| Cores | 1C1Q, 2C2Q, 3C3Q |
| QAT | Not Used |
| Command Line (AES-GCM-128) | `./build/ipsec-secgw --lcores=40 -n 4 -w b7:00.0 -w b7:00.1 -vdev="crypto_aesni_gcm0,socket_id=1" -- -p 0x3 -u 1 -P -config="(0,0,40),(1,0,40)" -f ./ipsec_test_gcm.cfg` |

Test Result:

| AES-GCM-128 | 64 | 128 | 256 | 512 | 1024 | 1500 |
|---|---|---|---|---|---|---|
| 1C1Q | 4.924 | 4.442 | 3.728 | 2.764 | 1.928 | 1.572 |
| 2C2Q | 8.532 | 7.538 | 6.129 | 4.594 | 3.211 | 2.508 |
| 3C3Q | 12.738 | 11.405 | 9.731 | 7.58 | 4.592 | 3.224 |


IPSec Performance Test for AES-GCM-128 with Intel-IPSec-MB library
1C1Q
2C2Q
3C3Q
15
10
5
0
Throughput (MPPS)
64
128
256
512
1024
1500
Packet Size (Bytes)

**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 Dec.2 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/inteladvanced-encryption-standard-instructions-aes-ni/** Copyright © 2019 Intel Corporation. All rights reserved.

§