DPDK Intel Cryptodev Performance Report
Release 23.03

Test Date: Mar 29th, 2023
Author: Intel DPDK Validation team
# Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 29 2023</td>
<td>1.0</td>
<td>Initial document for release</td>
</tr>
</tbody>
</table>
Contents

Audience and Purpose.................................................................................................................................. 4
Cryptodev Test setup: .................................................................................................................................... 4

Intel® Xeon® Platinum 8180 Processor (38.5M Cache, 2.50 GHz) ......................................................... 6
  Hardware & Software Ingredients.................................................................................................................. 6
  Test Case 1 – Cryptodev QAT(Intel QuickAssist Technology) PMD performance test......................... 7
  Test Case 2 – Cryptodev SW (AESNI-MB, AESNI-GCM) PMD performance test ....................... 9

Intel® Xeon® Processor D-1553N (12M Cache, 2.30 GHz) ................................................................. 11
  Hardware & Software Ingredients.............................................................................................................. 11
  Test Case 3 – Cryptodev QAT(Intel QuickAssist Technology) PMD performance test.................. 12
  Test Case 4 – Cryptodev SW (AESNI-MB, AESNI-GCM) PMD performance test .................. 14
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.

Cryptodev 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](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. It is 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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Platform</td>
<td>PURLEY</td>
</tr>
<tr>
<td>Chipset</td>
<td>Intel® C620 Series Chipset</td>
</tr>
</tbody>
</table>
| CPU             | Intel(R) Xeon(R) Platinum 8180 CPU @ 2.50GHz  
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| Ubuntu 18.04.5 LTS (Bionic Beaver)                                                                                                                                                                             |
| BIOS            | SE5C620.86B.00.01.0009.101920170742                                                                                                                                                                           |
| Microcode version| 0x2006e05                                                                                                                                                                                                  |
| Linux kernel version | 5.4.0-144-generic                                                                                                                                                   |
| GCC version     | 7.5.0                                                                                                                                                                                                        |
| DPDK version    | 23.03                                                                                                                                                                                                       |
| ipsec-mb version | 1.3                                                                                                                                                                                                        |

## Boot and BIOS settings

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot settings</td>
<td>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</td>
</tr>
</tbody>
</table>
| BIOS            | CPU Power and Performance Policy <Performance>  
Package C-state Disabled  
Hardware P-state Disabled  
Enhanced Intel® Speedstep® Tech Disabled  
Intel® Turbo Boost Technology Disabled |
| DPDK Settings   | Build options: CC=gcc meson --werror -Denable_kmods=True -Dlibdir=lib --default-library=static x86_64-native-linuxapp-gcc |
Test Case 1 – Cryptodev QAT (Intel QuickAssist Technology) PMD performance test

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cores</td>
<td>3C6T</td>
</tr>
<tr>
<td>QAT</td>
<td>Integrated Intel QuickAssist Technology, PCI-e x16 Mode</td>
</tr>
</tbody>
</table>

Command line (AES-CBC-128/SHA1-HMAC)
```
./x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf --socket-mem 2048,0 --legacy-mem -a 0000:1a:01.0 -a 0000:1c:01.0 -a 0000:1e:01.0 -a 0000:1a:01.1 -a 0000:1c:01.1 -a 0000:1e:01.1 -a 0000:1a:01.2 -a 0000:1c:01.2 -a 0000:1e:01.2 -a 0000:1a:01.3 -a 0000:1c:01.3 -a 0000:1e:01.3 -a 0000:1a:01.4 -a 0000:1c:01.4 -a 0000:1e:01.4 -a 0000:1a:01.5 -a 0000:1c:01.5 -a 0000:1e:01.5 --vdev crypto_scheduler_pmd_1,worker=0000:1a:01.0_qat_sym,worker=0000:1c:01.0_qat_sym,worker=0000:1e:01.0_qat_sym,mode=round-robin --vdev crypto_scheduler_pmd_2,worker=0000:1a:01.1_qat_sym,worker=0000:1c:01.1_qat_sym,worker=0000:1e:01.1_qat_sym,mode=round-robin --vdev crypto_scheduler_pmd_3,worker=0000:1a:01.2_qat_sym,worker=0000:1c:01.2_qat_sym,worker=0000:1e:01.2_qat_sym,mode=round-robin --vdev crypto_scheduler_pmd_4,worker=0000:1a:01.3_qat_sym,worker=0000:1c:01.3_qat_sym,worker=0000:1e:01.3_qat_sym,mode=round-robin --vdev crypto_scheduler_pmd_5,worker=0000:1a:01.4_qat_sym,worker=0000:1c:01.4_qat_sym,worker=0000:1e:01.4_qat_sym,mode=round-robin --vdev crypto_scheduler_pmd_6,worker=0000:1a:01.5_qat_sym,worker=0000:1c:01.5_qat_sym,worker=0000:1e:01.5_qat_sym,mode=round-robin --vdev crypto_scheduler_pmd_7,worker=0000:1a:01.6_qat_sym,worker=0000:1c:01.6_qat_sym,worker=0000:1e:01.6_qat_sym,mode=round-robin --vdev crypto_scheduler_pmd_8,worker=0000:1a:01.7_qat_sym,worker=0000:1c:01.7_qat_sym,worker=0000:1e:01.7_qat_sym,mode=round-robin --vdev
```

Command line (AES-CBC-128/SHA2-256-HMAC)
```
./x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf --socket-mem 2048,0 --legacy-mem -a 0000:1a:01.0 -a 0000:1c:01.0 -a 0000:1e:01.0 -a 0000:1a:01.1 -a 0000:1c:01.1 -a 0000:1e:01.1 -a 0000:1a:01.2 -a 0000:1c:01.2 -a 0000:1e:01.2 -a 0000:1a:01.3 -a 0000:1c:01.3 -a 0000:1e:01.3 -a 0000:1a:01.4 -a 0000:1c:01.4 -a 0000:1e:01.4 -a 0000:1a:01.5 -a 0000:1c:01.5 -a 0000:1e:01.5 --vdev crypto_scheduler_pmd_1,worker=0000:1a:01.0_qat_sym,worker=0000:1c:01.0_qat_sym,worker=0000:1e:01.0_qat_sym,mode=round-robin --vdev crypto_scheduler_pmd_2,worker=0000:1a:01.1_qat_sym,worker=0000:1c:01.1_qat_sym,worker=0000:1e:01.1_qat_sym,mode=round-robin --vdev crypto_scheduler_pmd_3,worker=0000:1a:01.2_qat_sym,worker=0000:1c:01.2_qat_sym,worker=0000:1e:01.2_qat_sym,mode=round-robin --vdev crypto_scheduler_pmd_4,worker=0000:1a:01.3_qat_sym,worker=0000:1c:01.3_qat_sym,worker=0000:1e:01.3_qat_sym,mode=round-robin --vdev crypto_scheduler_pmd_5,worker=0000:1a:01.4_qat_sym,worker=0000:1c:01.4_qat_sym,worker=0000:1e:01.4_qat_sym,mode=round-robin --vdev crypto_scheduler_pmd_6,worker=0000:1a:01.5_qat_sym,worker=0000:1c:01.5_qat_sym,worker=0000:1e:01.5_qat_sym,mode=round-robin --vdev crypto_scheduler_pmd_7,worker=0000:1a:01.6_qat_sym,worker=0000:1c:01.6_qat_sym,worker=0000:1e:01.6_qat_sym,mode=round-robin --vdev crypto_scheduler_pmd_8,worker=0000:1a:01.7_qat_sym,worker=0000:1c:01.7_qat_sym,worker=0000:1e:01.7_qat_sym,mode=round-robin --vdev
```

Command line (AES-GCM-128)
```
./x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf --socket-mem 2048,0 --legacy-mem -a 0000:1a:01.0 -a 0000:1c:01.0 -a 0000:1e:01.0 -a 0000:1a:01.1 -a 0000:1c:01.1 -a 0000:1e:01.1 -a 0000:1a:01.2 -a 0000:1c:01.2 -a 0000:1e:01.2 -a 0000:1a:01.3 -a 0000:1c:01.3 -a 0000:1e:01.3 -a 0000:1a:01.4 -a 0000:1c:01.4 -a 0000:1e:01.4 -a 0000:1a:01.5 -a 0000:1c:01.5 -a 0000:1e:01.5 --vdev crypto_scheduler_pmd_1,worker=0000:1a:01.0_qat_sym,worker=0000:1c:01.0_qat_sym,worker=0000:1e:01.0_qat_sym,mode=round-robin --vdev crypto_scheduler_pmd_2,worker=0000:1a:01.1_qat_sym,worker=0000:1c:01.1_qat_sym,worker=0000:1e:01.1_qat_sym,mode=round-robin --vdev crypto_scheduler_pmd_3,worker=0000:1a:01.2_qat_sym,worker=0000:1c:01.2_qat_sym,worker=0000:1e:01.2_qat_sym,mode=round-robin --vdev crypto_scheduler_pmd_4,worker=0000:1a:01.3_qat_sym,worker=0000:1c:01.3_qat_sym,worker=0000:1e:01.3_qat_sym,mode=round-robin --vdev crypto_scheduler_pmd_5,worker=0000:1a:01.4_qat_sym,worker=0000:1c:01.4_qat_sym,worker=0000:1e:01.4_qat_sym,mode=round-robin --vdev crypto_scheduler_pmd_6,worker=0000:1a:01.5_qat_sym,worker=0000:1c:01.5_qat_sym,worker=0000:1e:01.5_qat_sym,mode=round-robin --vdev crypto_scheduler_pmd_7,worker=0000:1a:01.6_qat_sym,worker=0000:1c:01.6_qat_sym,worker=0000:1e:01.6_qat_sym,mode=round-robin --vdev crypto_scheduler_pmd_8,worker=0000:1a:01.7_qat_sym,worker=0000:1c:01.7_qat_sym,worker=0000:1e:01.7_qat_sym,mode=round-robin --vdev
```
For the maximum possible QAT performance in the multi-core system, the workers are mapped on QAT instance one by one and the round-robin scheduler mode is configured.

### Test Result:

<table>
<thead>
<tr>
<th>Buffer Size (Bytes)</th>
<th>AES-CBC-128/SHA1-HMAC (Gbps)</th>
<th>AES-CBC-128/SHA2-256-HMAC (Gbps)</th>
<th>AES-GCM-128 (Gbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>64</td>
<td>9.50</td>
<td>9.39</td>
<td>8.27</td>
</tr>
<tr>
<td>128</td>
<td>18.70</td>
<td>18.54</td>
<td>16.40</td>
</tr>
<tr>
<td>256</td>
<td>35.89</td>
<td>35.58</td>
<td>31.73</td>
</tr>
<tr>
<td>512</td>
<td>63.24</td>
<td>62.71</td>
<td>57.50</td>
</tr>
<tr>
<td>1024</td>
<td>85.45</td>
<td>83.37</td>
<td>79.97</td>
</tr>
<tr>
<td>2048</td>
<td>91.70</td>
<td>92.47</td>
<td>91.85</td>
</tr>
</tbody>
</table>
Test Case 2 – Cryptodev SW (AESNI-MB, AESNI-GCM) PMD performance test

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cores</td>
<td>1C1T</td>
</tr>
<tr>
<td>QAT</td>
<td>Not used</td>
</tr>
<tr>
<td>Command line (AES-CBC-128/SHA1-HMAC)</td>
<td>./x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf --socket-mem 2048,0 --legacy-mem --udev 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</td>
</tr>
<tr>
<td>Command line (AES-CBC-128/SHA2-256-HMAC)</td>
<td>./x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf --socket-mem 2048,0 --legacy-mem --udev crypto_aesni_gcm_pmd_1 -l 9,10 -n 6 -- --buffer-sz 64,128,256,512,1024,2048 --optype aead --ptest throughput -- auth-key-sz 64 --cipher-key-sz 16 --devtype crypto_aesni_gcm --aead-op encrypt --burst-sz 32 --total-ops 10000000 --silent -- digest-sz 16 --aead-algo sha2-256-hmac --cipher-algo aes-cbc --cipher-op encrypt</td>
</tr>
<tr>
<td>Command line (AES-GCM-128)</td>
<td>./x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf --socket-mem 2048,0 --legacy-mem --udev 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 1000000 --silent -- digest-sz 16 --aead-algo aes-gcm --aead-iv-sz 12</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Buffer Size (Bytes)</th>
<th>AES-CBC-128/SHA1-HMAC (Gbps)</th>
<th>AES-CBC-128/SHA2-256-HMAC (Gbps)</th>
<th>AES-GCM-128 (Gbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>64</td>
<td>4.37</td>
<td>3.55</td>
<td>10.22</td>
</tr>
<tr>
<td>128</td>
<td>7.44</td>
<td>5.95</td>
<td>14.77</td>
</tr>
<tr>
<td>256</td>
<td>11.61</td>
<td>9.05</td>
<td>21.94</td>
</tr>
<tr>
<td>512</td>
<td>16.14</td>
<td>12.26</td>
<td>28.85</td>
</tr>
<tr>
<td>1024</td>
<td>19.99</td>
<td>14.89</td>
<td>34.24</td>
</tr>
<tr>
<td>2048</td>
<td>22.79</td>
<td>16.68</td>
<td>37.85</td>
</tr>
</tbody>
</table>
Cryptodev SW (AESNI-MB, AESNI-GCM) PMD performance test

Throughput (Gbps) vs Buffer Size (Bytes)

- 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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Platform</td>
<td>GRANGEVILLE</td>
</tr>
<tr>
<td>CPU</td>
<td>Intel® Xeon® Processor D-1553N (12M Cache, 2.30 GHz)</td>
</tr>
<tr>
<td></td>
<td>[link](<a href="https://ark.intel.com/products/123002/Intel-Xeon-Processor-D-1553N-12M-">https://ark.intel.com/products/123002/Intel-Xeon-Processor-D-1553N-12M-</a></td>
</tr>
<tr>
<td></td>
<td>Cache-2.30-GHz)</td>
</tr>
<tr>
<td></td>
<td>Number of cores 8, Number of threads 16.</td>
</tr>
<tr>
<td>Memory</td>
<td>Total 65536 MBs over 4 channels @ 2400 MHz</td>
</tr>
<tr>
<td>Operating System</td>
<td>Ubuntu 18.04.5 LTS (Bionic Beaver)</td>
</tr>
<tr>
<td>BIOS</td>
<td>GNUVTR1.26B.0010.DS1.1706230411</td>
</tr>
<tr>
<td>Microcode version</td>
<td>0xe000014</td>
</tr>
<tr>
<td>Linux kernel version</td>
<td>5.4.0-144-generic</td>
</tr>
<tr>
<td>GCC version</td>
<td>9.4.0</td>
</tr>
<tr>
<td>DPDK version</td>
<td>23.03</td>
</tr>
<tr>
<td>ipsec-mb version</td>
<td>1.3</td>
</tr>
</tbody>
</table>

Boot and BIOS settings

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot settings</td>
<td>intel_iommu=on iommu=pt intel_pstate=disable isolcpus=4-7,12-15 ncp nthz_full=4-7,12-15 rcu_nobs=4-7,12-15 hugepagesz=1G hugepages=10 default_hugepagesz=1G</td>
</tr>
</tbody>
</table>
| BIOS               | Boot performance mode <Max Performance>
|                    | CPU C state Disabled
|                    | Energy efficient P-state Disabled
|                    | Turbo Mode Disabled |
| DPDK Settings      | Build options: CC=gcc meson --werror -Denable_kmods=True -Dlibdir=lib --default-|
|                    | library=static x86_64-native-linuxapp-gcc |
Test Case 3 – Cryptodev QAT(Intel QuickAssist Technology) PMD performance test

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cores</td>
<td>2C4T</td>
</tr>
<tr>
<td>QAT</td>
<td>Integrated Intel QuickAssist Technology</td>
</tr>
<tr>
<td>Command line</td>
<td>./x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf --socket-mem 2048,0 --legacy-mem -a 0000:02:01.0 -a 0000:02:01.1 -a 0000:02:01.2 -a 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 shal-hmac --cipher-algo aes-cbc --cipher-op encrypt</td>
</tr>
<tr>
<td>Command line</td>
<td>./x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf --socket-mem 2048,0 --legacy-mem -a 0000:02:01.0 -a 0000:02:01.1 -a 0000:02:01.2 -a 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</td>
</tr>
<tr>
<td>Command line</td>
<td>./x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf --socket-mem 2048,0 --legacy-mem -a 0000:02:01.0 -a 0000:02:01.1 -a 0000:02:01.2 -a 0000:02:01.3 -l 4,5,13,6,14 -n 4 -- --aesd-key-sz 16 --buffer-sz 64,128,256,512,1024,2048 --optype aead --ptest throughput --aesd-aad-sz 16 --devtype crypto_qat --aesd-op encrypt --burst-sz 32 --total-ops 30000000 --silent --digest-sz 16 --aesd-algo aes-gcm --aesd-iv-sz 12</td>
</tr>
<tr>
<td>Notes</td>
<td>For the maximum possible QAT performance in the multi-core system, the workers are mapped on QAT instance one by one and the round-robin scheduler mode is configured</td>
</tr>
</tbody>
</table>

Test Result:

<table>
<thead>
<tr>
<th>Buffer Size (Bytes)</th>
<th>AES-CBC-128/SHA1-HMAC (Gbps)</th>
<th>AES-CBC-128/SHA2-256-HMAC (Gbps)</th>
<th>AES-GCM-128 (Gbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>64</td>
<td>3.90</td>
<td>3.89</td>
<td>3.35</td>
</tr>
<tr>
<td>128</td>
<td>7.72</td>
<td>7.68</td>
<td>6.66</td>
</tr>
<tr>
<td>256</td>
<td>15.06</td>
<td>14.92</td>
<td>13.10</td>
</tr>
<tr>
<td>512</td>
<td>28.31</td>
<td>27.99</td>
<td>24.69</td>
</tr>
<tr>
<td>1024</td>
<td>45.60</td>
<td>46.67</td>
<td>39.58</td>
</tr>
<tr>
<td>2048</td>
<td>52.70</td>
<td>52.45</td>
<td>49.85</td>
</tr>
</tbody>
</table>
Cryptodev QAT (Intel QuickAssist Technology)
PMD performance test
Test Case 4 – Cryptodev SW (AESNI-MB, AESNI-GCM) PMD performance test

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cores</td>
<td>1C1T</td>
</tr>
<tr>
<td>QAT</td>
<td>Not used</td>
</tr>
<tr>
<td>Command line (AES-CBC-128/SHA1-HMAC)</td>
<td>./x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf --socket-mem 2048,0 --legacy-mem --vdev crypto_aesni_mb_pmd_1 -l 4,5 -n 4 -- --buffer-size 64,128,256,512,1024,2048 --optype cipher-then-auth --ptest throughput --auth-key-size 64 --cipher-key-size 16 --devtype crypto_aesni_mb --cipher-iv-size 16 --auth-op generate --burst-size 32 --total-ops 1000000 --silent --digest-size 12 --auth-algo sha1-hmac --cipher-algo aes-cbc --cipher-op encrypt</td>
</tr>
<tr>
<td>Command line (AES-CBC-128/SHA2-256-HMAC)</td>
<td>./x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf --socket-mem 2048,0 --legacy-mem --vdev crypto_aesni_gcm_pmd_1 -l 4,5 -n 4 -- --aead-key-size 64,128,256,512,1024,2048 --optype aead --ptest throughput --aead-key-size 64 --cipher-key-size 16 --devtype crypto_aesni_gcm --aead-iv-size 16 --auth-op generate --aead-iv-size 12 --total-ops 10000000 --silent --aead-algo sha2-256-hmac --aead-algo aes-gcm --aead-op encrypt</td>
</tr>
<tr>
<td>Command line (AES-GCM-128)</td>
<td>./x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf --socket-mem 2048,0 --legacy-mem --vdev crypto_aesni_gcm_pmd_1 -l 4,5 -n 4 -- --aead-key-size 16 --buffer-size 64,128,256,512,1024,2048 --optype aead --ptest throughput --aead-aad-size 16 --devtype crypto_aesni_gcm --aead-op encrypt --burst-size 32 --total-ops 1000000 --silent --digest-size 16 --aead-algo sha1-hmac --aead-algo aes-gcm --aead-iv-size 12</td>
</tr>
<tr>
<td>Notes</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Buffer Size (Bytes)</th>
<th>AES-CBC-128/SHA1-HMAC (Gbps)</th>
<th>AES-CBC-128/SHA2-256-HMAC (Gbps)</th>
<th>AES-GCM-128 (Gbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>64</td>
<td>2.05</td>
<td>1.37</td>
<td>4.83</td>
</tr>
<tr>
<td>128</td>
<td>3.38</td>
<td>2.21</td>
<td>8.33</td>
</tr>
<tr>
<td>256</td>
<td>5.13</td>
<td>3.19</td>
<td>11.95</td>
</tr>
<tr>
<td>512</td>
<td>6.85</td>
<td>4.08</td>
<td>15.87</td>
</tr>
<tr>
<td>1024</td>
<td>8.23</td>
<td>4.75</td>
<td>18.87</td>
</tr>
<tr>
<td>2048</td>
<td>9.17</td>
<td>5.18</td>
<td>20.86</td>
</tr>
</tbody>
</table>
Cryptodev SW (AESNI-MB, AESNI-GCM) PMD performance test

Throughput (Gbps)

Buffer Size (Bytes)

- 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.

Performance results are based on testing as of Mar. 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 © 2023 Intel Corporation. All rights reserved.