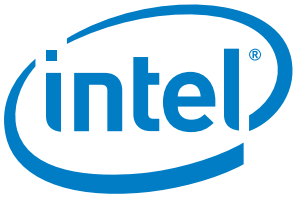

DPDK v25.11 Intel Cryptodev Performance Report

Test Date: March 2026

Author: Intel DPDK Validation team

Revision History

Date	Revision	Comment
09/02/2026	1.0	Initial document for release
06/03/2026	1.1	Review comments
23/04/2026	2.0	GNRD results update
28/04/2026	2.1	Minor updates

Contents

Figures

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 platform setup

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

- 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

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.

IPsec-mb library

https://github.com/intel/intel-ipsec-mb

Intel® Multi-Buffer Crypto for IPsec Library is a highly optimized software library designed to accelerate the core cryptographic operations used in IPsec. It delivers industry-leading performance across a wide range of Intel® processors by executing authentication and encryption workloads in parallel using multi-buffer processing techniques.

Test Platform Overview

4th Gen Intel® Xeon® Scalable Processors (Sapphire Rapids)

Item	Description
Server Platform	Intel® Xeon® Platinum 8468H Processor (105M Cache, 2.10 GHz)
Chipset	Intel® C620 Series Chipset
CPU	Number of cores 48, Number of threads 96.
Memory	DDR5 Total 65536 MBs over 2 channels @ 4800 MHz
PCIe	Gen 5.0 Max Lanes up 80
QAT	Product Name: 4xxx CPM 2.0 Gen 4
Operating System	Ubuntu24.04.4 LTS (Noble Numbat)
BIOS	02.00.00
Microcode version	0x2b000643
Boot settings	vfio-pci.disable_denylist=1 hugepagesz=1G hugepages=40 default_hugepagesz=1G isolcpus=1-26,97-122,48-74,144-170 intel_iommu=on nohz_full=1-26,97-122,48-74,144-170 rcu_nocbs=1-26,97-122,48-74,144-170 iommu=pt intel_pstate=disable numa_balancing=disable
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
Linux kernel version	6.8.0-90-generic
GCC version	13.3.0
DPDK version	25.11
DPDK menson settings	CC=gcc meson -Dlibdir=lib --default-library=static x86_64-native-linuxapp-gcc

Intel® Xeon® 6 processors (Granite Rapids-D)

Item	Description
Server Platform	Intel® Xeon® 6756P-B Processor (256M Cache, 2.20 GHz)
Chipset	Intel 531 PCH
CPU	Number of cores 64, Number of threads 128
Memory	DDR5 Total 384GB over 6 channels @ 6400 MT/s
PCIe	32 Lanes Gen 5; 16 Lanes Gen 4
QAT	Product Name: 420xx CPM 2.2 Gen 5
Operating System	Ubuntu24.04.4 LTS (Noble Numbat)
BIOS	KVLDCRB1.IPC.3038.P24.2602060842
Microcode version	0x010002f3
Boot settings	hugepagesz=1G hugepages=16 default_hugepagesz=1G isolcpus=1-15,37-51 intel_iommu=on iommu=pt nohz_full=1-15,37-51 rcu_nocbs=1-15,37-51 nmi_watchdog=0 audit=0 nosoftlockup processor.max_cstate=0 intel_idle.max_cstate=0 hpet=disable mce=off tsc=reliable numa_balancing=disable intel_pstate=disable nomodeset
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 SNC(Sub-NUMA Clustering) Enabled
Linux kernel version	6.8.0-110-generic
GCC version	13.3.0
DPDK version	25.11
DPDK menson settings	CC=gcc meson -Dlibdir=lib --default-library=static x86_64-native-linuxapp-gcc

Crypto Algorithms Covered

IPsec Algorithms (4th Gen Xeon)

- AES-CBC-128/SHA2-256-HMAC
- AES-GCM-128-GCM-128
- AES-GCM-256-GCM-256
- ChaCha20-Poly1305-Poly1305

The performance of the above standard IPsec algorithms is measured and captured on a 4th Gen Intel® Xeon® SoC (Sapphire Rapids). The evaluation uses Intel® QuickAssist Technology via the DPDK QAT PMD, as well as the Intel® IPsec Multi-Buffer library through the DPDK AESNI_MB PMD.

Sapphire Rapids is selected as the reference platform because QAT performance on this generation is mature and stable, this SoC should provide a consistent and reliable baseline for IPsec crypto performance characterization.

Wireless Algorithms (6th Gen Xeon)

- SNOW3G-UEA2 / SNOW3G-UIA2
- ZUC-EEA3 / ZUC-EIA3
- AES-CTR-CMAC

The performance of the above standard wireless security algorithms is measured and captured on a 6th Gen Intel® Xeon® SoC (Granite Rapids-D). The evaluation is conducted using Intel® QuickAssist Technology via the DPDK QAT PMD, as well as the Intel® IPsec Multi-Buffer library through the DPDK AESNI_MB PMD.

Granite Rapids-D is chosen due to QAT's newly introduced wireless acceleration slice, which provides native hardware support for industry-standard wireless algorithms and reflects current market requirements.

Performance Tuning and Test Configuration Notes

This section describes the key performance-related configuration choices and limitations relevant to the crypto performance evaluation. These notes provide context for the test results and document constraints that influence scalability and queue utilization.

CPU Core Utilization and Scheduling

For optimal performance, crypto-perf testing typically requires two or more CPU cores to fully saturate the available crypto device queues. In some test configuration used here, core 9 is designated as the main (scheduler) core, while core 10 operates as a worker core responsible for enqueue and dequeue operations with the crypto device. This configuration is marked as 1C1T test case.

During multicore testing, the DPDK crypto-perf application does not have visibility into which CPU cores are actually used by the Poll Mode Driver (PMD). Due to this limitation, crypto-perf restricts each crypto device to a single queue pair. This design choice avoids the risk of oversubscribing CPU resources, but it also limits the application's ability to scale across multiple queues even when additional cores are available.

QAT VF Queue Configuration

The QAT Virtual Function (VF) device configuration file includes the NumberCyInstances parameter, which defines how many QAT crypto queue pairs are exposed per VF at the kernel level. Under normal circumstances, increasing this value would allow DPDK applications to utilize multiple crypto queues per VF.

However, because dpdk_crypto_perf is limited to using only one queue pair per crypto device, increasing NumberCyInstances does not provide any benefit in this test setup. As a result, NumberCyInstances effectively remains at its default value of 2 for QAT Gen 4, and additional queue pairs are not exercised by the application.

Buffer Size Semantics in crypto-perf

In dpdk_crypto_perf, the --buffer-sz parameter specifies the payload length passed to the cryptodev for processing. For combined cipher-then-authentication operations, the same buffer length is used for both encryption and authentication. This means that the full payload defined by --buffer-sz is encrypted and subsequently authenticated.

Understanding this behavior is important when interpreting performance results, as buffer size directly impacts both cryptographic workload and throughput measurements.

IMIX Selection and Block Size Alignment

A classical IMIX profile is used to measure crypto buffer processing performance. However, for AES-CBC-128 with SHA2-HMAC, input buffers must be a multiple of the cipher block size. Therefore, the IMIX values were adjusted to 64, 576, and 1328 bytes to satisfy block size alignment requirements.

Test Methodology & Results

Section 1. IPsec Algorithms

Test Case 1 – Cryptodev QAT PMD performance test -1C1T

Item	Description
Test Case	Cryptodev performance for AES-CBC-128/SHA2-256-HMAC , AES-GCM-128, AES-GCM-256, ChaCha20-Poly1305 with Intel QuickAssist Technology
Cores	1C1T
QAT	Product Name: 4xxx, 4 QAT devices enabled
QAT dev conf settings	ServicesEnabled=sym NumberCyInstances = 2 NumberDcInstances = 2
Command line (AES-CBC-128/SHA2-256-HMAC)	`x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:6b:00.1,qat_legacy_capa=1 --socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,2048,4096 --devtype crypto_qat --optype cipher-then-auth --cipher-algo aes-cbc --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo sha2-256-hmac --auth-op generate --auth-key-sz 64 --digest-sz 32 --desc-nb=256`  `x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:6b:00.1,qat_legacy_capa=1 --socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,576,1328 --imix 28,16,4 --devtype crypto_qat --optype cipher-then-auth --cipher-algo aes-cbc --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo sha2-256-hmac --auth-op generate --auth-key-sz 64 --digest-sz 32 --desc-nb=256`
Command line (AES-GCM-128)	`x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:6b:00.1,qat_legacy_capa=1 --socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,1500,2048,4096 --devtype crypto_qat --optype aead --aead-algo aes-gcm --aead-op encrypt --aead-key-sz 16 --aead-iv-sz 12 --aead-aad-sz 16 --digest-sz 16 --desc-nb=256`  `x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:6b:00.1,qat_legacy_capa=1 --socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,590,1514 --imix 28,16,4 --devtype crypto_qat --optype aead --aead-algo aes-gcm --aead-op encrypt --aead-key-sz 16 --aead-iv-sz 12 --aead-aad-sz 16 --digest-sz 16 --desc-nb=256`
Command line (AES-GCM-256)	`x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:6b:00.1,qat_legacy_capa=1 --socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,1500,2048,4096 --devtype crypto_qat --optype aead --aead-algo aes-gcm --aead-op encrypt --aead-key-sz 32 --aead-iv-sz 12 --aead-aad-sz 32 --digest-sz 16 --desc-nb=256`

	`x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:6b:00.1,qat_legacy_capa=1 --socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,590,1514 --imix 28,16,4 --devtype crypto_qat --optype aead --aead-algo aes-gcm --aead-op encrypt --aead-key-sz 32 --aead-iv-sz 12 --aead-aad-sz 32 --digest-sz 16 --desc-nb=256`
Command line (ChaCha20-Poly1305)	`x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:6b:00.1,qat_legacy_capa=1 --socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,1500,2048,4096 --devtype crypto_qat --optype aead --aead-algo chacha20-poly1305 --aead-op encrypt --aead-key-sz 32 --aead-iv-sz 12 --aead-aad-sz 16 --digest-sz 16 --desc-nb=256`  `x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:6b:00.1,qat_legacy_capa=1 --socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,590,1514 --imix 28,16,4 --devtype crypto_qat --optype aead --aead-algo chacha20-poly1305 --aead-op encrypt --aead-key-sz 32 --aead-iv-sz 12 --aead-aad-sz 16 --digest-sz 16 --desc-nb=256`

Test Result (Measured on 4th Gen Xeon- Sapphire Rapids)

Buffer Size (Bytes)	AES-CBC-128/ SHA2-256-HMAC (Gbps)	AES-GCM-128 (Gbps)	AES-GCM-256 (Gbps)	ChaCha20-Poly1305 (Gbps)
64	2.14	2.61	2.61	2.61
256	8.50	10.41	10.40	10.43
512	16.92	20.69	20.66	20.71
1024	33.13	40.92	40.71	40.63
1500	n/a	58.98	58.27	57.67
2048	46.24	76.94	73.65	70.20
4096	52.35	92.39	90.87	84.23
IMIX	11.73	14.50	14.47	14.51

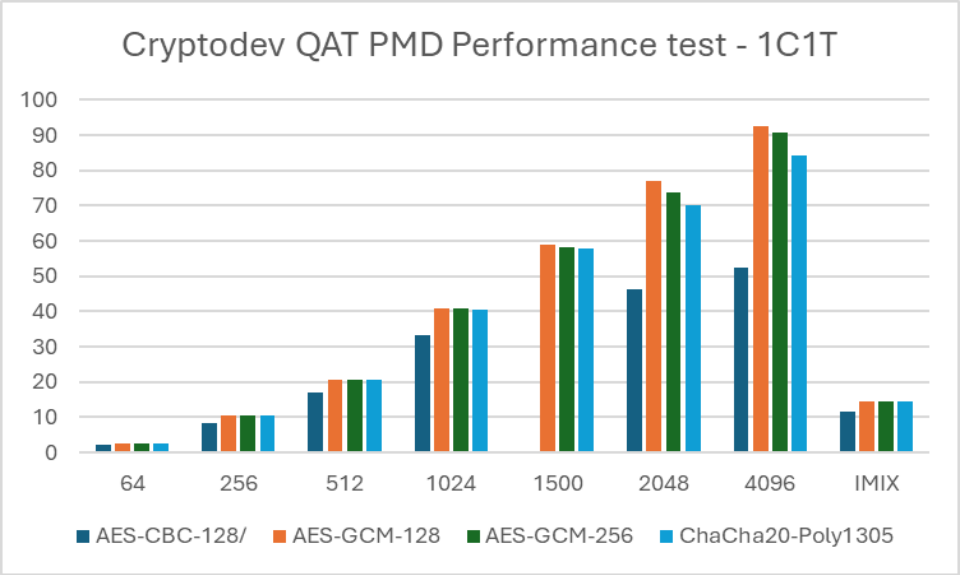

Figure 1 Cryptodev QAT PMD IPsec Algorithms 1C1T Perf

Test Case 2 - Cryptodev QAT PMD performance test-3C3T

Item	Description
Test Case	Cryptodev performance for AES-CBC-128/SHA2-256-HMAC , AES-GCM-128, AES-GCM-256, ChaCha20-Poly1305 with Intel QuickAssist Technology
Cores	3C3T
QAT	Product Name: 4xxx, 4 QAT devices enabled
QAT dev conf settings	ServicesEnabled=sym NumberCyInstances = 2 NumberDcInstances = 2

Command line (AES-CBC-128/SHA2-256-HMAC)	`x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11,12 \`
	`-a 0000:6b:00.1,qat_legacy_capa=1 -a 0000:70:00.1,qat_legacy_capa=1 -a`
	`0000:75:00.1,qat_legacy_capa=1 -a 0000:7a:00.1,qat_legacy_capa=1 \`
	`-a 0000:6b:00.2,qat_legacy_capa=1 -a 0000:70:00.2,qat_legacy_capa=1 -a`
	`0000:75:00.2,qat_legacy_capa=1 -a 0000:7a:00.2,qat_legacy_capa=1 \`
	`-a 0000:6b:00.3,qat_legacy_capa=1 -a 0000:70:00.3,qat_legacy_capa=1 -a`
	`0000:75:00.3,qat_legacy_capa=1 -a 0000:7a:00.3,qat_legacy_capa=1 \`
	`--vdev`
	`crypto_scheduler_0,worker=0000:6b:00.1_qat_sym,worker=0000:70:00.1_qat_sym,wo`
	`rker=0000:75:00.1_qat_sym,worker=0000:7a:00.1_qat_sym,mode=round-robin \`
	`--vdev`
	`crypto_scheduler_1,worker=0000:6b:00.2_qat_sym,worker=0000:70:00.2_qat_sym,wo`
	`rker=0000:75:00.2_qat_sym,worker=0000:7a:00.2_qat_sym,mode=round-robin \`
	`--vdev`
	`crypto_scheduler_2,worker=0000:6b:00.3_qat_sym,worker=0000:70:00.3_qat_sym,wo`
	`rker=0000:75:00.3_qat_sym,worker=0000:7a:00.3_qat_sym,mode=round-robin \`
	`--socket-mem 2048,2048 -n 8  -- --ptest throughput --silent  --total-ops`
	`5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,2048,4096 \`
	`--devtype crypto_scheduler --optype cipher-then-auth --cipher-algo aes-cbc --`
	`cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 \`
	`--auth-algo sha2-256-hmac --auth-op generate --auth-key-sz 64 --digest-sz 32`
	`--pool-sz 10000 --desc-nb=256`
	
	`x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11,12 \`
	`-a 0000:6b:00.1,qat_legacy_capa=1 -a 0000:70:00.1,qat_legacy_capa=1 -a`
	`0000:75:00.1,qat_legacy_capa=1 -a 0000:7a:00.1,qat_legacy_capa=1 \`
	`-a 0000:6b:00.2,qat_legacy_capa=1 -a 0000:70:00.2,qat_legacy_capa=1 -a`
	`0000:75:00.2,qat_legacy_capa=1 -a 0000:7a:00.2,qat_legacy_capa=1 \`
	`-a 0000:6b:00.3,qat_legacy_capa=1 -a 0000:70:00.3,qat_legacy_capa=1 -a`
	`0000:75:00.3,qat_legacy_capa=1 -a 0000:7a:00.3,qat_legacy_capa=1 \`
	`--vdev`
	`crypto_scheduler_0,worker=0000:6b:00.1_qat_sym,worker=0000:70:00.1_qat_sym,wo`
	`rker=0000:75:00.1_qat_sym,worker=0000:7a:00.1_qat_sym,mode=round-robin \`
	`--vdev`
	`crypto_scheduler_1,worker=0000:6b:00.2_qat_sym,worker=0000:70:00.2_qat_sym,wo`
	`rker=0000:75:00.2_qat_sym,worker=0000:7a:00.2_qat_sym,mode=round-robin \`
	`--vdev`
	`crypto_scheduler_2,worker=0000:6b:00.3_qat_sym,worker=0000:70:00.3_qat_sym,wo`
	`rker=0000:75:00.3_qat_sym,worker=0000:7a:00.3_qat_sym,mode=round-robin \`
	`--socket-mem 2048,2048 -n 8  -- --ptest throughput --silent  --total-ops`
	`5000000 --burst-sz 32 --buffer-sz 64,576,1328 --imix 28,16,4 \`
	`--devtype crypto_scheduler --optype cipher-then-auth --cipher-algo aes-cbc --`
	`cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 \`
	`--auth-algo sha2-256-hmac --auth-op generate --auth-key-sz 64 --digest-sz 32`
	`--pool-sz 10000 --desc-nb=256`

Command line (AES-GCM-128)	x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11,12 \ -a 0000:6b:00.1,qat_legacy_capa=1 -a 0000:70:00.1,qat_legacy_capa=1 -a 0000:75:00.1,qat_legacy_capa=1 -a 0000:7a:00.1,qat_legacy_capa=1 \ -a 0000:6b:00.2,qat_legacy_capa=1 -a 0000:70:00.2,qat_legacy_capa=1 -a 0000:75:00.2,qat_legacy_capa=1 -a 0000:7a:00.2,qat_legacy_capa=1 \ -a 0000:6b:00.3,qat_legacy_capa=1 -a 0000:70:00.3,qat_legacy_capa=1 -a 0000:75:00.3,qat_legacy_capa=1 -a 0000:7a:00.3,qat_legacy_capa=1 \ --vdev crypto_scheduler_0,worker=0000:6b:00.1_qat_sym,worker=0000:70:00.1_qat_sym,worker=0000:75:00.1_qat_sym,worker=0000:7a:00.1_qat_sym,mode=round-robin \ --vdev crypto_scheduler_1,worker=0000:6b:00.2_qat_sym,worker=0000:70:00.2_qat_sym,worker=0000:75:00.2_qat_sym,worker=0000:7a:00.2_qat_sym,mode=round-robin \ --vdev crypto_scheduler_2,worker=0000:6b:00.3_qat_sym,worker=0000:70:00.3_qat_sym,worker=0000:75:00.3_qat_sym,worker=0000:7a:00.3_qat_sym,mode=round-robin \ --socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,1500,2048,4096 \ --devtype crypto_scheduler --optype aead --aead-algo aes-gcm --aead-op encrypt --aead-key-sz 16 --aead-iv-sz 12 --aead-aad-sz 16 --digest-sz 16 --pool-sz 10000 --desc-nb=256 x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11,12 \ -a 0000:6b:00.1,qat_legacy_capa=1 -a 0000:70:00.1,qat_legacy_capa=1 -a 0000:75:00.1,qat_legacy_capa=1 -a 0000:7a:00.1,qat_legacy_capa=1 \ -a 0000:6b:00.2,qat_legacy_capa=1 -a 0000:70:00.2,qat_legacy_capa=1 -a 0000:75:00.2,qat_legacy_capa=1 -a 0000:7a:00.2,qat_legacy_capa=1 \ -a 0000:6b:00.3,qat_legacy_capa=1 -a 0000:70:00.3,qat_legacy_capa=1 -a 0000:75:00.3,qat_legacy_capa=1 -a 0000:7a:00.3,qat_legacy_capa=1 \ --vdev crypto_scheduler_0,worker=0000:6b:00.1_qat_sym,worker=0000:70:00.1_qat_sym,worker=0000:75:00.1_qat_sym,worker=0000:7a:00.1_qat_sym,mode=round-robin \ --vdev crypto_scheduler_1,worker=0000:6b:00.2_qat_sym,worker=0000:70:00.2_qat_sym,worker=0000:75:00.2_qat_sym,worker=0000:7a:00.2_qat_sym,mode=round-robin \ --vdev crypto_scheduler_2,worker=0000:6b:00.3_qat_sym,worker=0000:70:00.3_qat_sym,worker=0000:75:00.3_qat_sym,worker=0000:7a:00.3_qat_sym,mode=round-robin \ --socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,590,1514 --imix 28,16,4 \ --devtype crypto_scheduler --optype aead --aead-algo aes-gcm --aead-op encrypt --aead-key-sz 16 --aead-iv-sz 12 --aead-aad-sz 16 --digest-sz 16 --pool-sz 10000 --desc-nb=256
Command line (AES-GCM-256)	x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11,12 \ -a 0000:6b:00.1,qat_legacy_capa=1 -a 0000:70:00.1,qat_legacy_capa=1 -a 0000:75:00.1,qat_legacy_capa=1 -a 0000:7a:00.1,qat_legacy_capa=1 \ -a 0000:6b:00.2,qat_legacy_capa=1 -a 0000:70:00.2,qat_legacy_capa=1 -a 0000:75:00.2,qat_legacy_capa=1 -a 0000:7a:00.2,qat_legacy_capa=1 \ -a 0000:6b:00.3,qat_legacy_capa=1 -a 0000:70:00.3,qat_legacy_capa=1 -a 0000:75:00.3,qat_legacy_capa=1 -a 0000:7a:00.3,qat_legacy_capa=1 \ --vdev crypto_scheduler_0,worker=0000:6b:00.1_qat_sym,worker=0000:70:00.1_qat_sym,worker=0000:75:00.1_qat_sym,worker=0000:7a:00.1_qat_sym,mode=round-robin \

	`--vdev crypto_scheduler_1,worker=0000:6b:00.2_qat_sym,worker=0000:70:00.2_qat_sym,worker=0000:75:00.2_qat_sym,worker=0000:7a:00.2_qat_sym,mode=round-robin \`
	`--vdev crypto_scheduler_2,worker=0000:6b:00.3_qat_sym,worker=0000:70:00.3_qat_sym,worker=0000:75:00.3_qat_sym,worker=0000:7a:00.3_qat_sym,mode=round-robin \`
	`--socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,1500,2048,4096 \`
	`--devtype crypto_scheduler --optype aead --aead-algo aes-gcm --aead-op encrypt --aead-key-sz 32 --aead-iv-sz 12 --aead-aad-sz 32 --digest-sz 16 --pool-sz 10000 --desc-nb=256`
	
	`x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11,12 \`
	`-a 0000:6b:00.1,qat_legacy_capa=1 -a 0000:70:00.1,qat_legacy_capa=1 -a 0000:75:00.1,qat_legacy_capa=1 -a 0000:7a:00.1,qat_legacy_capa=1 \`
	`-a 0000:6b:00.2,qat_legacy_capa=1 -a 0000:70:00.2,qat_legacy_capa=1 -a 0000:75:00.2,qat_legacy_capa=1 -a 0000:7a:00.2,qat_legacy_capa=1 \`
	`-a 0000:6b:00.3,qat_legacy_capa=1 -a 0000:70:00.3,qat_legacy_capa=1 -a 0000:75:00.3,qat_legacy_capa=1 -a 0000:7a:00.3,qat_legacy_capa=1 \`
	`--vdev crypto_scheduler_0,worker=0000:6b:00.1_qat_sym,worker=0000:70:00.1_qat_sym,worker=0000:75:00.1_qat_sym,worker=0000:7a:00.1_qat_sym,mode=round-robin \`
	`--vdev crypto_scheduler_1,worker=0000:6b:00.2_qat_sym,worker=0000:70:00.2_qat_sym,worker=0000:75:00.2_qat_sym,worker=0000:7a:00.2_qat_sym,mode=round-robin \`
	`--vdev crypto_scheduler_2,worker=0000:6b:00.3_qat_sym,worker=0000:70:00.3_qat_sym,worker=0000:75:00.3_qat_sym,worker=0000:7a:00.3_qat_sym,mode=round-robin \`
	`--socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,590,1514 --imix 28,16,4 \`
	`--devtype crypto_scheduler --optype aead --aead-algo aes-gcm --aead-op encrypt --aead-key-sz 32 --aead-iv-sz 12 --aead-aad-sz 32 --digest-sz 16 --pool-sz 10000 --desc-nb=256`

Command line
(ChaCha20-Poly1305)
	`x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11,12 \`
	`-a 0000:6b:00.1,qat_legacy_capa=1 -a 0000:70:00.1,qat_legacy_capa=1 -a 0000:75:00.1,qat_legacy_capa=1 -a 0000:7a:00.1,qat_legacy_capa=1 \`
	`-a 0000:6b:00.2,qat_legacy_capa=1 -a 0000:70:00.2,qat_legacy_capa=1 -a 0000:75:00.2,qat_legacy_capa=1 -a 0000:7a:00.2,qat_legacy_capa=1 \`
	`-a 0000:6b:00.3,qat_legacy_capa=1 -a 0000:70:00.3,qat_legacy_capa=1 -a 0000:75:00.3,qat_legacy_capa=1 -a 0000:7a:00.3,qat_legacy_capa=1 \`
	`--vdev crypto_scheduler_0,worker=0000:6b:00.1_qat_sym,worker=0000:70:00.1_qat_sym,worker=0000:75:00.1_qat_sym,worker=0000:7a:00.1_qat_sym,mode=round-robin \`
	`--vdev crypto_scheduler_1,worker=0000:6b:00.2_qat_sym,worker=0000:70:00.2_qat_sym,worker=0000:75:00.2_qat_sym,worker=0000:7a:00.2_qat_sym,mode=round-robin \`
	`--vdev crypto_scheduler_2,worker=0000:6b:00.3_qat_sym,worker=0000:70:00.3_qat_sym,worker=0000:75:00.3_qat_sym,worker=0000:7a:00.3_qat_sym,mode=round-robin \`
	`--socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,1500,2048,4096 \`
	`--devtype crypto_scheduler --optype aead --aead-algo chacha20-poly1305 --aead-op encrypt --aead-key-sz 32 --aead-iv-sz 12 --aead-aad-sz 16 --digest-sz`

	16 --pool-sz 10000 --desc-nb=256 x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11,12 \ -a 0000:6b:00.1,qat_legacy_capa=1 -a 0000:70:00.1,qat_legacy_capa=1 -a 0000:75:00.1,qat_legacy_capa=1 -a 0000:7a:00.1,qat_legacy_capa=1 \ -a 0000:6b:00.2,qat_legacy_capa=1 -a 0000:70:00.2,qat_legacy_capa=1 -a 0000:75:00.2,qat_legacy_capa=1 -a 0000:7a:00.2,qat_legacy_capa=1 \ -a 0000:6b:00.3,qat_legacy_capa=1 -a 0000:70:00.3,qat_legacy_capa=1 -a 0000:75:00.3,qat_legacy_capa=1 -a 0000:7a:00.3,qat_legacy_capa=1 \ --vdev crypto_scheduler_0,worker=0000:6b:00.1_qat_sym,worker=0000:70:00.1_qat_sym,worker=0000:75:00.1_qat_sym,worker=0000:7a:00.1_qat_sym,mode=round-robin \ --vdev crypto_scheduler_1,worker=0000:6b:00.2_qat_sym,worker=0000:70:00.2_qat_sym,worker=0000:75:00.2_qat_sym,worker=0000:7a:00.2_qat_sym,mode=round-robin \ --vdev crypto_scheduler_2,worker=0000:6b:00.3_qat_sym,worker=0000:70:00.3_qat_sym,worker=0000:75:00.3_qat_sym,worker=0000:7a:00.3_qat_sym,mode=round-robin \ --socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,590,1514 --imix 28,16,4 \ --devtype crypto_scheduler --optype aead --aead-algo chacha20-poly1305 --aead-op encrypt --aead-key-sz 32 --aead-iv-sz 12 --aead-aad-sz 16 --digest-sz 16 --pool-sz 10000 --desc-nb=256

Test Result (Measured on 4th Gen Xeon- Sapphire Rapids)

Buffer Size (Bytes)	AES-CBC-128/ SHA2-256-HMAC (Gbps)	AES-GCM-128 (Gbps)	AES-GCM-256 (Gbps)	ChaCha20-Poly1305 (Gbps)
64	7.45	7.20	7.20	10.44
256	30.17	28.27	28.22	41.61
512	61.63	55.25	55.31	82.57
1024	123.04	110.70	113.83	162.24
1500	n/a	168.08	170.15	228.30
2048	184.89	231.29	228.72	273.67
4096	209.32	342.80	356.87	336.95
IMIX	46.17	39.40	42.31	57.94

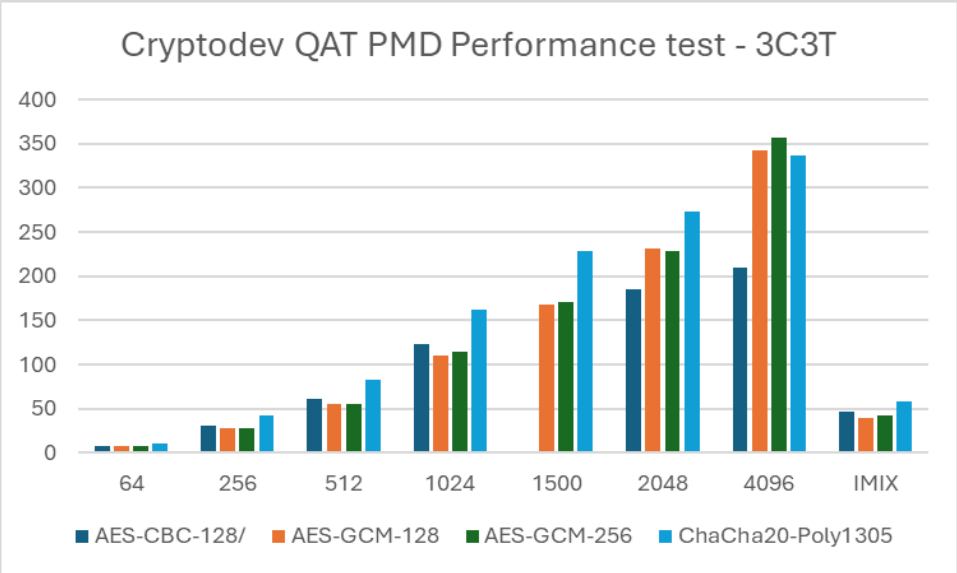

Figure 2 Cryptodev QAT PMD IPsec Algorithms 3C3T Perf

Test Case 3 – Cryptodev AESNI-MB PMD performance test -1C1T

Item	Description
Test Case	Cryptodev performance for AES-CBC-128/SHA2-256-HMAC, AES-GCM-128, AES-GCM-256, ChaCha20-Poly1305, SNOW3G-UEA2/SNOW3G-UIA2, ZUC-EEA3/ZUC-EIA3 with Intel AESNI_MB PMD
Cores	1C1T
Intel IPsec-mb	V2.0.1
Command line (AES-CBC-128/SHA2-256-HMAC)	`x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:00:00.0 --vdev crypto_aesni_mb_pmd0 --socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,2048,4096 --devtype crypto_aesni_mb --optype cipher-then-auth --cipher-algo aes-cbc --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo sha2-256-hmac --auth-op generate --auth-key-sz 64 --digest-sz 16`  `x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:00:00.0 --vdev crypto_aesni_mb_pmd0 --socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,576,1328 --imix 28,16,4 --devtype crypto_aesni_mb --optype cipher-then-auth --cipher-algo aes-cbc --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo sha2-256-hmac --auth-op generate --auth-key-sz 64 --digest-sz 16`
Command line (AES-GCM-128)	`x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:00:00.0 --vdev crypto_aesni_gcm_pmd0 --socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,1500,2048,4096 --devtype crypto_aesni_gcm --optype aead --aead-algo aes-gcm --aead-op encrypt --aead-key-sz 16 --aead-iv-sz 12 --aead-aad-sz 16 --digest-sz 16`  `x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:00:00.0 --vdev crypto_aesni_gcm_pmd0 --socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,590,1514 --imix 28,16,4 --devtype crypto_aesni_gcm --optype aead --aead-algo aes-gcm --aead-op encrypt --aead-key-sz 16 --aead-iv-sz 12 --aead-aad-sz 16 --digest-sz 16`
Command line (AES-GCM-256)	`x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:00:00.0 --vdev crypto_aesni_gcm_pmd0 --socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,590,1514 --imix 28,16,4 --devtype crypto_aesni_gcm --optype aead --aead-algo aes-gcm --aead-op encrypt --aead-key-sz 32 --aead-iv-sz 12 --aead-aad-sz 32 --digest-sz 16`  `x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:00:00.0 --vdev crypto_aesni_gcm_pmd0 --socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,590,1514 --imix 28,16,4 --devtype crypto_aesni_gcm --optype aead --aead-algo aes-gcm --aead-op encrypt --aead-key-sz 32 --aead-iv-sz 12 --aead-aad-sz 32 --digest-sz 16`
Command line (ChaCha20-Poly1305)	`x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:00:00.0 --vdev crypto_aesni_mb_pmd0 --socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,1500,2048,4096 --devtype crypto_aesni_mb --optype aead --aead-algo chacha20-poly1305 --aead-op encrypt --aead-key-sz 32 --aead-iv-sz 12 --aead-aad-sz 16 --digest-sz 16`

	`x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:00:00.0 --vdev crypto_aesni_mb_pmd0 --socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,590,1514 --imix 28,16,4 --devtype crypto_aesni_mb --optype aead --aead-algo chacha20-poly1305 --aead-op encrypt --aead-key-sz 32 --aead-iv-sz 12 --aead-aad-sz 16 --digest-sz 16`

Test Result (Measured on 4th Gen Xeon- Sapphire Rapids)

Buffer Size (Bytes)	AES-CBC-128/ SHA2-256-HMAC (Gbps)	AES-GCM-128 (Gbps)	AES-GCM-256 (Gbps)	ChaCha20-Poly1305 (Gbps)
64	2.70	13.65	12.37	2.42
256	7.00	34.94	30.66	6.14
512	9.47	51.74	45.78	8.89
1024	12.04	64.11	54.87	12.82
1500	n/a	73.26	58.59	13.92
2048	13.60	82.00	63.82	15.71
4096	14.63	91.27	69.36	18.64
IMIX	6.33	39.02	34.60	7.85

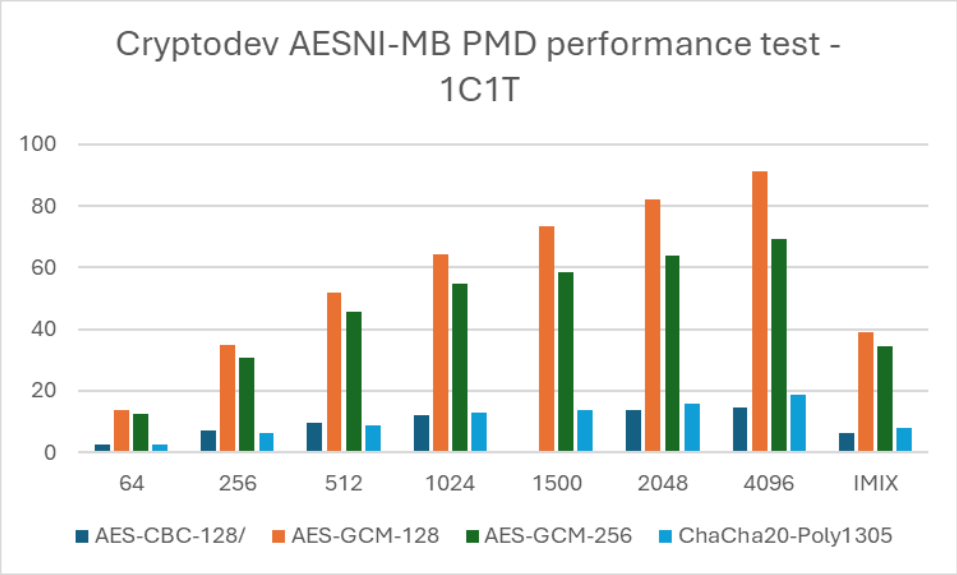

Figure 3 Cryptodev AESNI-MB PMD IPsec Algorithms 1C1T Perf

Test Case 4 – Cryptodev AESNI-MB PMD performance test -3C3T

Item	Description
Test Case	Cryptodev performance for AES-CBC-128/SHA2-256-HMAC , AES-GCM-128, AES-GCM-256, ChaCha20-Poly1305 with Intel AESNI_MB PMD
Cores	3C3T
Intel IPsec-mb	V2.0.1

Command line (AES-CBC-128/SHA2-256-HMAC)	`x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11,12 -a 0000:00:00.0 \`
	`--vdev crypto_aesni_mb_pmd1 --vdev crypto_aesni_mb_pmd2 --vdev crypto_aesni_mb_pmd3 \`
	`--vdev crypto_scheduler0,worker=crypto_aesni_mb_pmd1,mode=round-robin \`
	`--vdev crypto_scheduler1,worker=crypto_aesni_mb_pmd2,mode=round-robin \`
	`--vdev crypto_scheduler2,worker=crypto_aesni_mb_pmd3,mode=round-robin \`
	`--socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,2048,4096 \`
	`--devtype crypto_scheduler --optype cipher-then-auth --cipher-algo aes-cbc --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 \`
	`--auth-algo sha2-256-hmac --auth-op generate --auth-key-sz 64 --digest-sz 32 --pool-sz 10000 --desc-nb=256`
	
	`x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11,12 -a 0000:00:00.0 \`
	`--vdev crypto_aesni_mb_pmd1 --vdev crypto_aesni_mb_pmd2 --vdev crypto_aesni_mb_pmd3 \`
	`--vdev crypto_scheduler0,worker=crypto_aesni_mb_pmd1,mode=round-robin \`
	`--vdev crypto_scheduler1,worker=crypto_aesni_mb_pmd2,mode=round-robin \`
	`--vdev crypto_scheduler2,worker=crypto_aesni_mb_pmd3,mode=round-robin \`
	`--socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 \`
	`--buffer-sz 64,576,1328 --imix 28,16,4 \`
	`--devtype crypto_scheduler --optype cipher-then-auth --cipher-algo aes-cbc --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 \`
	`--auth-algo sha2-256-hmac --auth-op generate --auth-key-sz 64 --digest-sz 32 --pool-sz 10000 --desc-nb=256`

Command line (AES-GCM-128)	`x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11,12 -a 0000:00:00.0 \`
	`--vdev crypto_aesni_mb_pmd1 --vdev crypto_aesni_mb_pmd2 --vdev crypto_aesni_mb_pmd3 \`
	`--vdev crypto_scheduler0,worker=crypto_aesni_mb_pmd1,mode=round-robin \`
	`--vdev crypto_scheduler1,worker=crypto_aesni_mb_pmd2,mode=round-robin \`
	`--vdev crypto_scheduler2,worker=crypto_aesni_mb_pmd3,mode=round-robin \`
	`--socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,1500,2048,4096 \`
	`--devtype crypto_scheduler --optype aead --aead-algo aes-gcm --aead-op encrypt --aead-key-sz 16 --aead-iv-sz 12 --aead-aad-sz 16 --digest-sz 16 --pool-sz 10000 --desc-nb=256`
	
	`x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11,12 -a 0000:00:00.0 \`
	`--vdev crypto_aesni_mb_pmd1 --vdev crypto_aesni_mb_pmd2 --vdev crypto_aesni_mb_pmd3 \`
	`--vdev crypto_scheduler0,worker=crypto_aesni_mb_pmd1,mode=round-robin \`
	`--vdev crypto_scheduler1,worker=crypto_aesni_mb_pmd2,mode=round-robin \`
	`--vdev crypto_scheduler2,worker=crypto_aesni_mb_pmd3,mode=round-robin \`
	`--socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops`

	5000000 --burst-sz 32 \ --buffer-sz 64,590,1514 --imix 28,16,4 \ --devtype crypto_scheduler --optype aead --aead-algo aes-gcm --aead-op encrypt --aead-key-sz 16 --aead-iv-sz 12 --aead-aad-sz 16 --digest-sz 16 --pool-sz 10000 --desc-nb=256
Command line (AES-GCM-256)	x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11,12 -a 0000:00:00.0 \ --vdev crypto_aesni_mb_pmd1 --vdev crypto_aesni_mb_pmd2 --vdev crypto_aesni_mb_pmd3 \ --vdev crypto_scheduler0,worker=crypto_aesni_mb_pmd1,mode=round-robin \ --vdev crypto_scheduler1,worker=crypto_aesni_mb_pmd2,mode=round-robin \ --vdev crypto_scheduler2,worker=crypto_aesni_mb_pmd3,mode=round-robin \ --socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,1500,2048,4096 \ --devtype crypto_scheduler --optype aead --aead-algo aes-gcm --aead-op encrypt --aead-key-sz 32 --aead-iv-sz 12 --aead-aad-sz 32 --digest-sz 16 --pool-sz 10000 --desc-nb=256 x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11,12 -a 0000:00:00.0 \ --vdev crypto_aesni_mb_pmd1 --vdev crypto_aesni_mb_pmd2 --vdev crypto_aesni_mb_pmd3 \ --vdev crypto_scheduler0,worker=crypto_aesni_mb_pmd1,mode=round-robin \ --vdev crypto_scheduler1,worker=crypto_aesni_mb_pmd2,mode=round-robin \ --vdev crypto_scheduler2,worker=crypto_aesni_mb_pmd3,mode=round-robin \ --socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 \ --buffer-sz 64,590,1514 --imix 28,16,4 \ --devtype crypto_scheduler --optype aead --aead-algo aes-gcm --aead-op encrypt --aead-key-sz 32 --aead-iv-sz 12 --aead-aad-sz 32 --digest-sz 16 --pool-sz 10000 --desc-nb=256
Command line (ChaCha20-Poly1305)	x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11,12 -a 0000:00:00.0 \ --vdev crypto_aesni_mb_pmd1 --vdev crypto_aesni_mb_pmd2 --vdev crypto_aesni_mb_pmd3 \ --vdev crypto_scheduler0,worker=crypto_aesni_mb_pmd1,mode=round-robin \ --vdev crypto_scheduler1,worker=crypto_aesni_mb_pmd2,mode=round-robin \ --vdev crypto_scheduler2,worker=crypto_aesni_mb_pmd3,mode=round-robin \ --socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,1500,2048,4096 \ --devtype crypto_scheduler --optype aead --aead-algo chacha20-poly1305 --aead-op encrypt --aead-key-sz 32 --aead-iv-sz 12 --aead-aad-sz 16 --digest-sz 16 --pool-sz 10000 --desc-nb=256 x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11,12 -a 0000:00:00.0 \ --vdev crypto_aesni_mb_pmd1 --vdev crypto_aesni_mb_pmd2 --vdev crypto_aesni_mb_pmd3 \ --vdev crypto_scheduler0,worker=crypto_aesni_mb_pmd1,mode=round-robin \ --vdev crypto_scheduler1,worker=crypto_aesni_mb_pmd2,mode=round-robin \

	--vdev crypto_scheduler2,worker=crypto_aesni_mb_pmd3,mode=round-robin \ --socket-mem 2048,2048 -n 8 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 \ --buffer-sz 64,590,1514 --imix 28,16,4 \ --devtype crypto_scheduler --optype aead --aead-algo chacha20-poly1305 --aead-op encrypt --aead-key-sz 32 --aead-iv-sz 12 --aead-aad-sz 16 --digest-sz 16 --pool-sz 10000 --desc-nb=256

Test Result (Measured on 4th Gen Xeon- Sapphire Rapids)

Buffer Size (Bytes)	AES-CBC-128/ SHA2-256-HMAC (Gbps)	AES-GCM-128 (Gbps)	AES-GCM-256 (Gbps)	ChaCha20-Poly1305 (Gbps)
64	7.89	34.32	31.73	7.02
256	20.64	91.86	79.21	18.22
512	28.05	128.49	108.20	26.41
1024	35.90	181.03	150.50	38.27
1500	n/a	195.58	161.89	41.50
2048	40.63	227.76	180.98	47.03
4096	43.81	260.65	201.92	55.74
IMIX	18.95	103.35	93.24	23.20

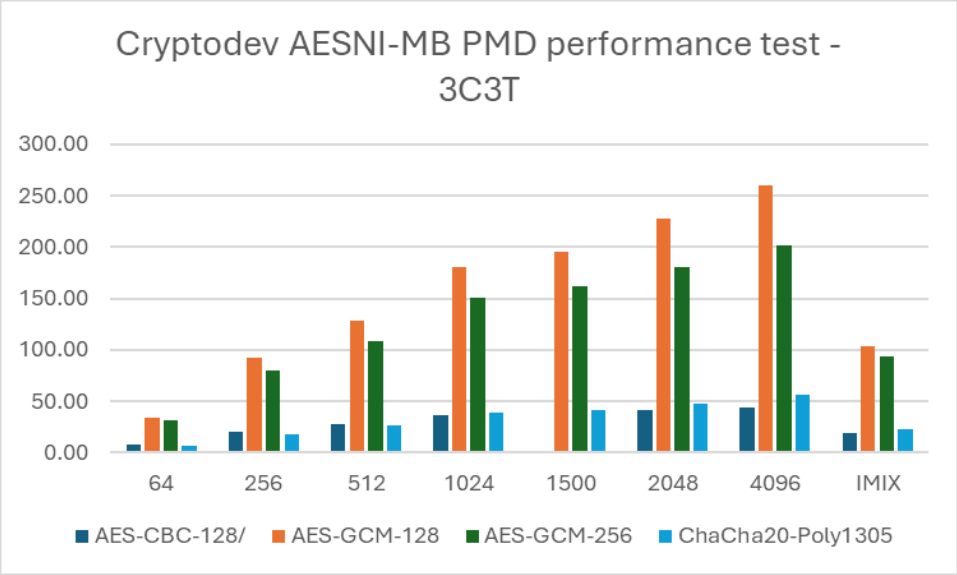

Figure 4 Cryptodev AESNI-MB PMD IPsec Algorithms 3C3T Perf

Section 2. Wireless Algorithms

Test Case 5 – Cryptodev QAT PMD performance test -1C1T

Item	Description
Test Case	Cryptodev performance for SNOW3G (cipher + auth), ZUC (cipher + auth) and AES-CBC-CMAC with Intel QuickAssist Technology
Cores	1C1T
QAT	Product Name: 420xx, 2 QAT devices enabled
QAT dev conf settings	ServicesEnabled=sym NumAsymAccelUnits = 0 NumSymAccelUnits = 4 NumDcAccelUnits = 0
Command line (SNOW3G (cipher + auth))	`x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:05:00.1,qat_legacy_capa=1 -n 8 --socket-mem 2048,0 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,1500,2048,4096 --devtype crypto_qat --optype cipher-then-auth --cipher-algo snow3g-uea2 --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo snow3g-uia2 --auth-op generate --auth-key-sz 16 --auth-iv-sz 16 --digest-sz 4 --desc-nb=256`  `x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:05:00.1,qat_legacy_capa=1 -n 8 --socket-mem 2048,0 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,590,1514 --imix 28,16,4 --devtype crypto_qat --optype cipher-then-auth --cipher-algo snow3g-uea2 --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo snow3g-uia2 --auth-op generate --auth-key-sz 16 --auth-iv-sz 16 --digest-sz 4 --desc-nb=256`
Command line (ZUC (cipher + auth))	`x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:05:00.1,qat_legacy_capa=1 -n 8 --socket-mem 2048,0 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,1500,2048,4096 --devtype crypto_qat --optype cipher-then-auth --cipher-algo zuc-eea3 --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo zuc-eia3 --auth-op generate --auth-key-sz 16 --auth-iv-sz 16 --digest-sz 4 --desc-nb=256`  `x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:05:00.1,qat_legacy_capa=1 -n 8 --socket-mem 2048,0 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,590,1514 --imix 28,16,4 --devtype crypto_qat --optype cipher-then-auth --cipher-algo zuc-eea3 --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo zuc-eia3 --auth-op generate --auth-key-sz 16 --auth-iv-sz 16 --digest-sz 4 --desc-nb=256`
Command line (AES-CTR-CMAC)	`x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:05:00.1,qat_legacy_capa=1 -n 8 --socket-mem 2048,0 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,1500,2048,4096 --devtype crypto_qat --optype cipher-then-auth --cipher-algo aes-ctr --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo aes-cmac --auth-op generate --auth-key-sz 16 --digest-sz 16 --desc-nb=256`

	x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:05:00.1,qat_legacy_capa=1 -n 8 --socket-mem 2048,0 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,590,1514 --imix 28,16,4 --devtype crypto_qat --optype cipher-then-auth --cipher-algo aes-ctr --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo aes-cmac --auth-op generate --auth-key-sz 16 --digest-sz 16 --desc-nb=256

Test Result (Measured on 6th Gen Xeon- Granite Rapids-D)

Buffer Size (Bytes)	SNOW3G (UEA2 + UIA2) (Gbps)	ZUC (EEA3 + EIA3) (Gbps)	AES-CTR +CMAC (Gbps)
64	3.89	4.04	4.14
256	15.15	15.97	16.37
512	29.84	31.46	32.33
1024	58.92	62.21	63.88
1500	84.84	89.92	88.91
2048	113.28	117.23	117.03
4096	163.52	167.81	174.94
IMIX	21.45	22.60	23.18

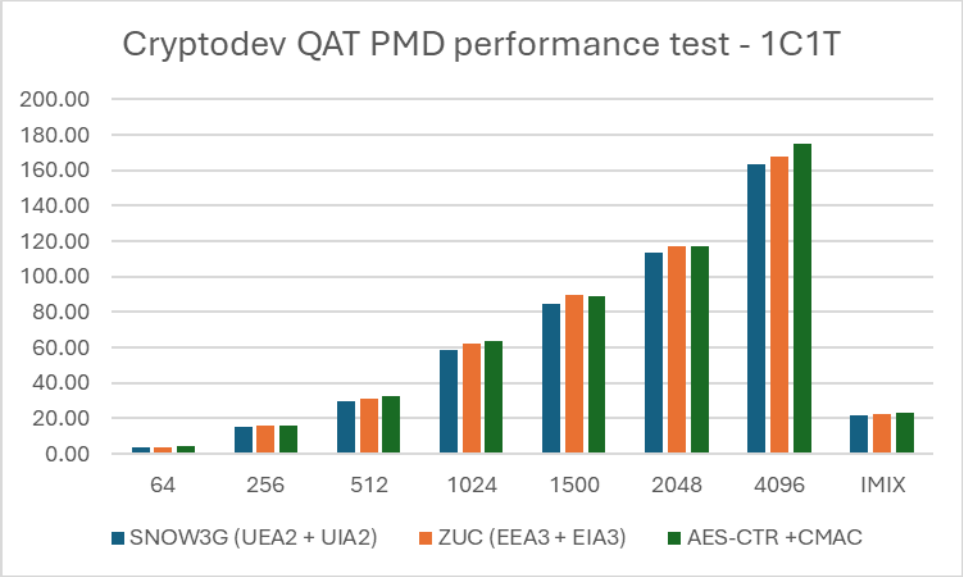

Figure 5 Cryptodev QAT PMD Wireless Algorithms 1C1T Perf

Test Case 6 – Cryptodev QAT PMD performance test-2C2T

Item	Description
Test Case	Cryptodev performance for SNOW3G (cipher + auth), ZUC (cipher + auth) and AES-CBC-CMAC with Intel QuickAssist Technology
Cores	2C2T
QAT	Product Name: 420xx, 2 QAT devices enabled
QAT dev conf settings	ServicesEnabled=sym NumAsymAccelUnits = 0 NumSymAccelUnits = 4 NumDcAccelUnits = 0
Command line (SNOW3G (cipher + auth))	x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11 --socket-mem 2048,0 -n 8 -a 0000:01:00.1,qat_legacy_capa=1 -a 0000:01:00.2,qat_legacy_capa=1 -a 0000:05:00.1,qat_legacy_capa=1 -a 0000:05:00.2,qat_legacy_capa=1 --vdev crypto_scheduler_0,worker=0000:01:00.1_qat_sym,worker=0000:05:00.1_qat_sym,mode=round-robin --vdev crypto_scheduler_1,worker=0000:01:00.2_qat_sym,worker=0000:05:00.2_qat_sym,mode=round-robin -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,1500,2048,4096 --devtype crypto_scheduler --optype cipher-then-auth --cipher-algo snow3g-uea2 --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo snow3g-uia2 --auth-op generate --auth-key-sz 16 --auth-iv-sz 16 --digest-sz 4 --pool-sz 10000 --desc-nb=256 x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11 --socket-mem 2048,0 -n 8 -a 0000:01:00.1,qat_legacy_capa=1 -a 0000:01:00.2,qat_legacy_capa=1 -a 0000:05:00.1,qat_legacy_capa=1 -a 0000:05:00.2,qat_legacy_capa=1 --vdev crypto_scheduler_0,worker=0000:01:00.1_qat_sym,worker=0000:05:00.1_qat_sym,mode=round-robin --vdev crypto_scheduler_1,worker=0000:01:00.2_qat_sym,worker=0000:05:00.2_qat_sym,mode=round-robin -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,590,1514 --imix 28,16,4 --devtype crypto_scheduler --optype cipher-then-auth --cipher-algo snow3g-uea2 --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo snow3g-uia2 --auth-op generate --auth-key-sz 16 --auth-iv-sz 16 --digest-sz 4 --pool-sz 10000 --desc-nb=256
Command line (ZUC (cipher + auth))	x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11 --socket-mem 2048,0 -n 8 -a 0000:01:00.1,qat_legacy_capa=1 -a 0000:01:00.2,qat_legacy_capa=1 -a 0000:05:00.1,qat_legacy_capa=1 -a 0000:05:00.2,qat_legacy_capa=1 --vdev crypto_scheduler_0,worker=0000:01:00.1_qat_sym,worker=0000:05:00.1_qat_sym,mode=round-robin --vdev crypto_scheduler_1,worker=0000:01:00.2_qat_sym,worker=0000:05:00.2_qat_sym,mode=round-robin -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,1500,2048,4096 --devtype crypto_scheduler --optype cipher-then-auth --cipher-algo zuc-eea3 --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo zuc-eia3 --auth-op generate --auth-key-sz 16 --auth-iv-sz 16 --digest-sz 4 --pool-sz 10000 --desc-nb=256 x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11 --socket-mem 2048,0 -n 8 -a 0000:01:00.1,qat_legacy_capa=1 -a 0000:01:00.2,qat_legacy_capa=1 -a 0000:05:00.1,qat_legacy_capa=1 -a

	0000:05:00.2,qat_legacy_capa=1 --vdev crypto_scheduler_0,worker=0000:01:00.1_qat_sym,worker=0000:05:00.1_qat_sym,mode=round-robin --vdev crypto_scheduler_1,worker=0000:01:00.2_qat_sym,worker=0000:05:00.2_qat_sym,mode=round-robin -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,590,1514 --imix 28,16,4 --devtype crypto_scheduler --optype cipher-then-auth --cipher-algo zuc-eea3 --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo zuc-eia3 --auth-op generate --auth-key-sz 16 --auth-iv-sz 16 --digest-sz 4 --pool-sz 10000 --desc-nb=256
Command line (AES-CTR-CMAC)	x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11 --socket-mem 2048,0 -n 8 -a 0000:01:00.1,qat_legacy_capa=1 -a 0000:01:00.2,qat_legacy_capa=1 -a 0000:05:00.1,qat_legacy_capa=1 -a 0000:05:00.2,qat_legacy_capa=1 --vdev crypto_scheduler_0,worker=0000:01:00.1_qat_sym,worker=0000:05:00.1_qat_sym,mode=round-robin --vdev crypto_scheduler_1,worker=0000:01:00.2_qat_sym,worker=0000:05:00.2_qat_sym,mode=round-robin -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,1500,2048,4096 --devtype crypto_scheduler --optype cipher-then-auth --cipher-algo aes-ctr --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo aes-cmac --auth-op generate --auth-key-sz 16 --digest-sz 16 --pool-sz 10000 --desc-nb=256 x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11 --socket-mem 2048,0 -n 8 -a 0000:01:00.1,qat_legacy_capa=1 -a 0000:01:00.2,qat_legacy_capa=1 -a 0000:05:00.1,qat_legacy_capa=1 -a 0000:05:00.2,qat_legacy_capa=1 --vdev crypto_scheduler_0,worker=0000:01:00.1_qat_sym,worker=0000:05:00.1_qat_sym,mode=round-robin --vdev crypto_scheduler_1,worker=0000:01:00.2_qat_sym,worker=0000:05:00.2_qat_sym,mode=round-robin -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,590,1514 --imix 28,16,4 --devtype crypto_scheduler --optype cipher-then-auth --cipher-algo aes-ctr --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo aes-cmac --auth-op generate --auth-key-sz 16 --digest-sz 16 --pool-sz 10000 --desc-nb=256

Test Result (Measured on 6th Gen Xeon- Granite Rapids-D)

Buffer Size (Bytes)	SNOW3G (UEA2 + UIA2) (Gbps)	ZUC (EEA3 + EIA3) (Gbps)	AES-CTR +CMAC (Gbps)
64	7.83	8.24	8.39
256	31.02	32.42	33.43
512	60.79	63.63	65.83
1024	116.42	125.20	129.18
1500	162.88	179.22	177.57
2048	219.43	228.16	233.16
4096	326.06	319.78	348.75
IMIX	43.04	45.94	47.02

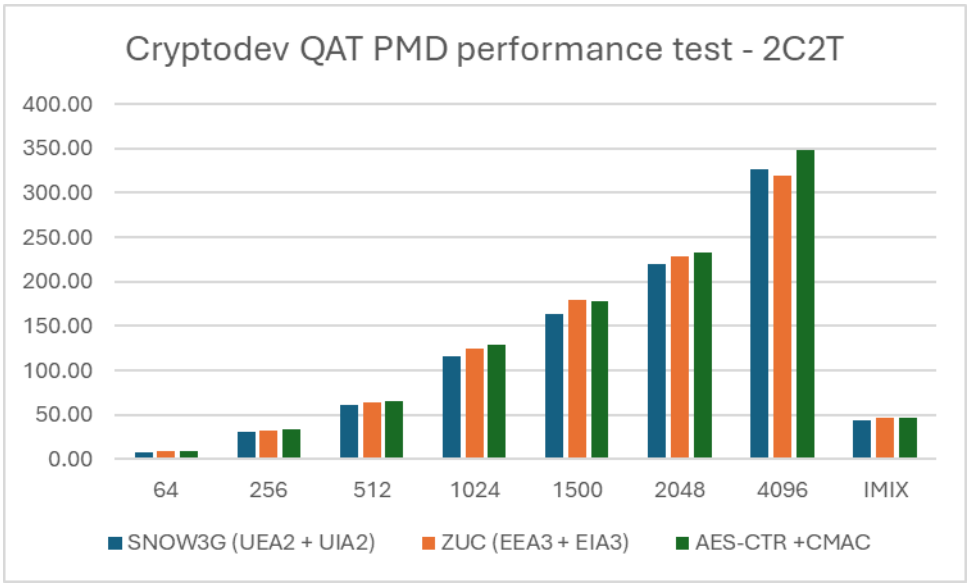

Figure 6 Cryptodev QAT PMD Wireless Algorithms 2C2T Perf

Test Case 7 – Cryptodev AESNI-MB PMD performance test -1C1T

Item	Description
Test Case	Cryptodev performance for SNOW3G (cipher + auth), ZUC (cipher + auth) and AES-CBC-CMAC with Intel AESNI_MB PMD
Cores	1C1T
intel-ipsec-mb	V2.0.1
Command line (SNOW3G (cipher + auth))	x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:00:00.0 --vdev crypto_aesni_mb_pmd0 -n 8 --socket-mem 2048,0 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,1500,2048,4096 --devtype crypto_aesni_mb --optype cipher-then-auth --cipher-algo snow3g-uea2 --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo snow3g-uia2 --auth-op generate --auth-key-sz 16 --auth-iv-sz 16 --digest-sz 4 --desc-nb=256 x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:00:00.0 --vdev crypto_aesni_mb_pmd0 -n 8 --socket-mem 2048,0 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,590,1514 --imix 28,16,4 --devtype crypto_aesni_mb --optype cipher-then-auth --cipher-algo snow3g-uea2 --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo snow3g-uia2 --auth-op generate --auth-key-sz 16 --auth-iv-sz 16 --digest-sz 4 --desc-nb=256
Command line (ZUC (cipher + auth))	x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:00:00.0 --vdev crypto_aesni_mb_pmd0 -n 8 --socket-mem 2048,0 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,1500,2048,4096 --devtype crypto_aesni_mb --optype cipher-then-auth --cipher-algo zuc-eea3 --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo zuc-eia3 --auth-op generate --auth-key-sz 16 --auth-iv-sz 16 --digest-sz 4 --desc-nb=256 x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:00:00.0 --vdev crypto_aesni_mb_pmd0 -n 8 --socket-mem 2048,0 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,590,1514 --imix 28,16,4 --devtype crypto_aesni_mb --optype cipher-then-auth --cipher-algo zuc-eea3 --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo zuc-eia3 --auth-op generate --auth-key-sz 16 --auth-iv-sz 16 --digest-sz 4 --desc-nb=256
Command line (AES-CTR-CMAC)	x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:00:00.0 --vdev crypto_aesni_mb_pmd0 -n 8 --socket-mem 2048,0 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,1500,2048,4096 --devtype crypto_aesni_mb --optype cipher-then-auth --cipher-algo aes-ctr --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo aes-cmac --auth-op generate --auth-key-sz 16 --digest-sz 16 --desc-nb=256 x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10 -a 0000:00:00.0 --vdev crypto_aesni_mb_pmd0 -n 8 --socket-mem 2048,0 -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,590,1514 --imix 28,16,4 --devtype crypto_aesni_mb --optype cipher-then-auth --cipher-algo aes-ctr --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo aes-cmac --auth-op generate --auth-key-sz 16 --digest-sz 16 --desc-nb=256

Test Result (Measured on 6th Gen Xeon- Granite Rapids-D)

Buffer Size (Bytes)	SNOW3G (UEA2 + UIA2) (Gbps)	ZUC (EEA3 + EIA3) (Gbps)	AES-CTR +CMAC (Gbps)
64	2.06	2.16	7.60
256	6.52	5.29	22.34
512	9.93	6.96	32.65
1024	13.58	8.37	41.52
1500	15.12	8.81	43.50
2048	16.59	9.24	46.41
4096	18.69	9.78	50.25
IMIX	5.46	1.23	16.43

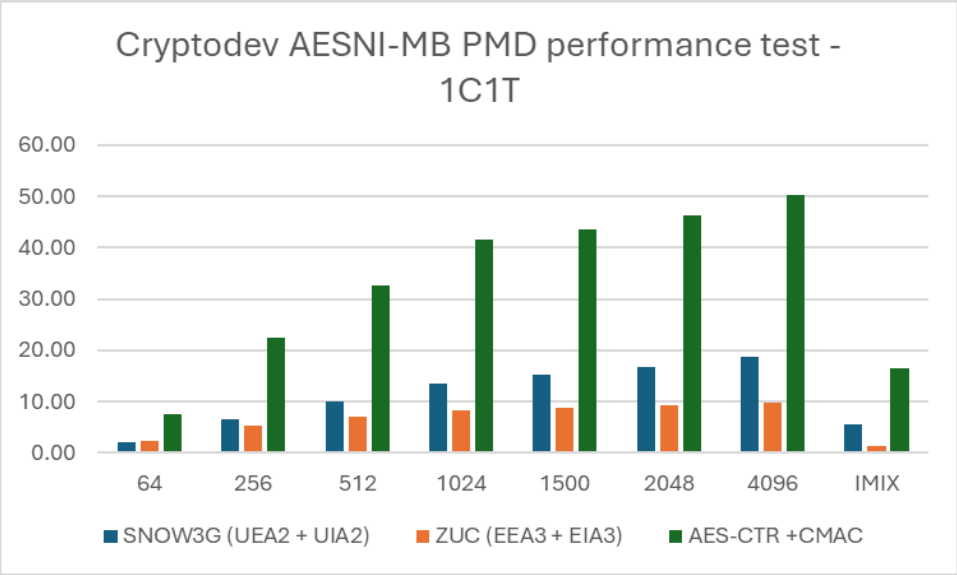

Figure 7 Cryptodev AESNI-MB PMD Wireless Algorithms 1C1T Perf

Test Case 8 – Cryptodev AESNI-MB PMD performance test -2C2T

Item	Description
Test Case	Cryptodev performance for SNOW3G (cipher + auth), ZUC (cipher + auth) and AES-CBC-CMAC with Intel AESNI_MB PMD
Cores	2C2T
intel-ipsec-mb	V2.0.1
Command line (SNOW3G (cipher + auth))	x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11 -a 0000:00:00.0 --socket-mem 2048,0 -n 8 --vdev crypto_aesni_mb_pmd1 --vdev crypto_aesni_mb_pmd2 --vdev crypto_scheduler_0,worker=crypto_aesni_mb_pmd1,mode=round-robin --vdev crypto_scheduler_1,worker=crypto_aesni_mb_pmd2,mode=round-robin -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,1500,2048,4096 --devtype crypto_scheduler --optype cipher-then-auth --cipher-algo snow3g-uea2 --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo snow3g-uia2 --auth-op generate --auth-key-sz 16 --auth-iv-sz 16 --digest-sz 4 --pool-sz 10000 --desc-nb=256 x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11 -a 0000:00:00.0 --socket-mem 2048,0 -n 8 --vdev crypto_aesni_mb_pmd1 --vdev crypto_aesni_mb_pmd2 --vdev crypto_scheduler_0,worker=crypto_aesni_mb_pmd1,mode=round-robin --vdev crypto_scheduler_1,worker=crypto_aesni_mb_pmd2,mode=round-robin -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,590,1514 --imix 28,16,4 --devtype crypto_scheduler --optype cipher-then-auth --cipher-algo snow3g-uea2 --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo snow3g-uia2 --auth-op generate --auth-key-sz 16 --auth-iv-sz 16 --digest-sz 4 --pool-sz 10000 --desc-nb=256
Command line (ZUC (cipher + auth))	x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11 -a 0000:00:00.0 --socket-mem 2048,0 -n 8 --vdev crypto_aesni_mb_pmd1 --vdev crypto_aesni_mb_pmd2 --vdev crypto_scheduler_0,worker=crypto_aesni_mb_pmd1,mode=round-robin --vdev crypto_scheduler_1,worker=crypto_aesni_mb_pmd2,mode=round-robin -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,1500,2048,4096 --devtype crypto_scheduler --optype cipher-then-auth --cipher-algo zuc-eea3 --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo zuc-eia3 --auth-op generate --auth-key-sz 16 --auth-iv-sz 16 --digest-sz 4 --pool-sz 10000 --desc-nb=256 x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11 -a 0000:00:00.0 --socket-mem 2048,0 -n 8 --vdev crypto_aesni_mb_pmd1 --vdev crypto_aesni_mb_pmd2 --vdev crypto_scheduler_0,worker=crypto_aesni_mb_pmd1,mode=round-robin --vdev crypto_scheduler_1,worker=crypto_aesni_mb_pmd2,mode=round-robin -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,590,1514 --imix 28,16,4 --devtype crypto_scheduler --optype cipher-then-auth --cipher-algo zuc-eea3 --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo zuc-eia3 --auth-op generate --auth-key-sz 16 --auth-iv-sz 16 --digest-sz 4 --pool-sz 10000 --desc-nb=256
Command line (AES-CTR-CMAC)	x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11 -a 0000:00:00.0 --socket-mem 2048,0 -n 8 --vdev crypto_aesni_mb_pmd1 --vdev crypto_aesni_mb_pmd2 --vdev crypto_scheduler_0,worker=crypto_aesni_mb_pmd1,mode=round-robin --vdev crypto_scheduler_1,worker=crypto_aesni_mb_pmd2,mode=round-robin -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,256,512,1024,1500,2048,4096 --devtype crypto_scheduler --optype cipher-then-auth --cipher-algo aes-ctr --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo aes-cmac --auth-op generate --auth-key-sz 16 --

	digest-sz 16 --desc-nb=256 x86_64-native-linuxapp-gcc/app/dpdk-test-crypto-perf -l 9,10,11 -a 0000:00:00.0 --socket-mem 2048,0 -n 8 --vdev crypto_aesni_mb_pmd1 --vdev crypto_aesni_mb_pmd2 --vdev crypto_scheduler_0,worker=crypto_aesni_mb_pmd1,mode=round-robin --vdev crypto_scheduler_1,worker=crypto_aesni_mb_pmd2,mode=round-robin -- --ptest throughput --silent --total-ops 5000000 --burst-sz 32 --buffer-sz 64,590,1514 --imix 28,16,4 --devtype crypto_scheduler --optype cipher-then-auth --cipher-algo aes-ctr --cipher-op encrypt --cipher-key-sz 16 --cipher-iv-sz 16 --auth-algo aes-cmac --auth-op generate --auth-key-sz 16 --digest-sz 16 --desc-nb=256

Test Result (Measured on 6th Gen Xeon- Granite Rapids-D)

Buffer Size (Bytes)	SNOW3G (UEA2 + UIA2) (Gbps)	ZUC (EEA3 + EIA3) (Gbps)	AES-CTR +CMAC (Gbps)
64	4.04	4.26	13.89
256	12.97	10.50	42.50
512	19.78	13.93	62.43
1024	26.89	16.63	80.82
1500	30.18	17.53	85.68
2048	33.14	18.43	92.01
4096	37.31	19.52	99.47
IMIX	10.69	2.44	32.41

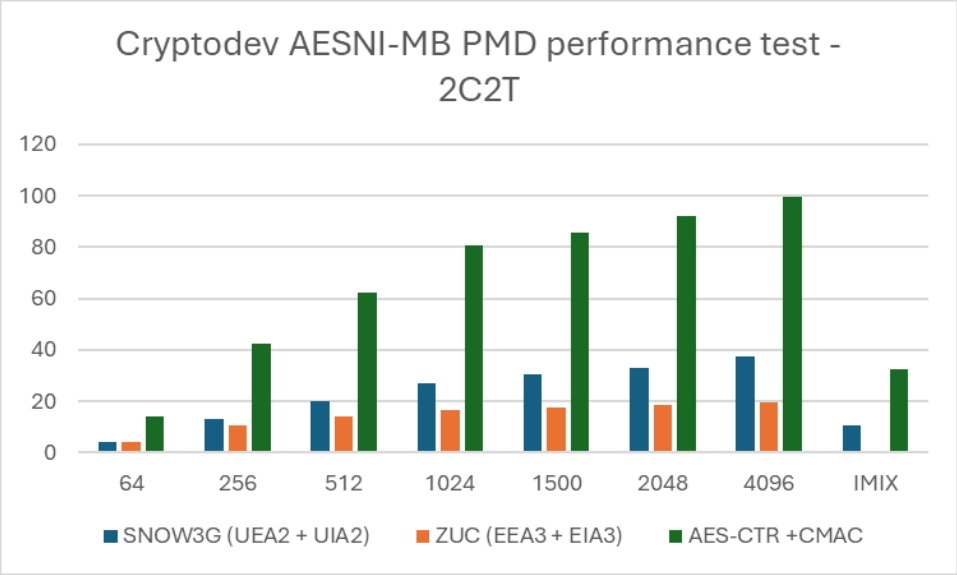

Figure 8 Cryptodev AESNI-MB PMD Wireless Algorithms 2C2T Perf

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 April 2026 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/**

§