A high performance framework for symmetric crypto packet processing in Data Plane Development Kit(DPDK)

DEEPAK KUMAR JAIN

INTEL, NETWORK PLATFORM GROUP

LEGAL DISCLAIMER

- No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.
- Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.
- This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest forecast, schedule, specifications and roadmaps.
- The products and services described may contain defects or errors known as errata which may cause deviations from published specifications. Current characterized errata are available on request.
- Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting: http://www.intel.com/design/literature.htm
- Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.
- *Other names and brands may be claimed as the property of others.
- Copyright © 2016, Intel Corporation. All rights reserved.
- Intel's compilers may or may not optimize to the same degree for non-Intel microprocessors for optimizations that are not unique to Intel microprocessors. These optimizations include SSE2, SSE3, and SSSE3 instruction sets and other optimizations. Intel does not guarantee the availability, functionality, or effectiveness of any optimization on microprocessors not manufactured by Intel. Microprocessor-dependent optimizations in this product are intended for use with Intel microprocessors. Certain optimizations not specific to Intel microarchitecture are reserved for Intel microprocessors. Please refer to the applicable product User and Reference Guides for more information regarding the specific instruction sets covered by this notice. Notice Revision #20110804
- Mileage may vary Disclaimer: 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** Test and System Configurations: Estimates are based on internal Intel analysis using atleast Data Plane Development Kit IpSec sample application on Intel(R) Xeon(R) CPU E5-2658 v4@ 2.30GHz with atleast using Intel(R) Communications Chipset(s) 8955 with Intel(R) QuickAssist Technology.

Agenda

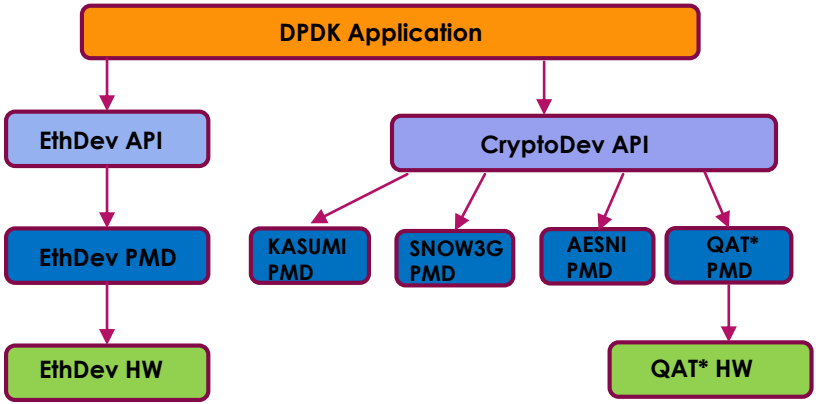
- About Cryptodev
- Current status
- Future features
- Hardware based Virtualization
- Performance
- Summary

Agenda

- **About Cryptodev**
- Current status
- Future features
- Hardware based Virtualization
- Performance
- Summary

About Cryptodev

- Crypto framework for processing symmetric crypto workloads in DPDK.
- Defines an API which supports both hardware accelerated lookaside (Intel® QuickAssist Technology) and software based crypto processing.
- Poll mode driver infrastructure for hardware and software crypto devices.
- Each PMD supports the **full cryptodev API**, but may only support a subset of all the possible algorithms/modes.
- Supports per device capabilities querying.



* QAT = Intel(R) QuickAssist Technology

About Cryptodev

DPDK

DPDK CRYPTODEV API COMPONENTS

- Device Management
- Device Capabilities
- Symmetric Algorithms Definitions
- Symmetric Session Management
- Queue Pair Management
- Device Statistics
- Operation Provisioning
- Operation Processing Enqueue/Dequeue

Agenda

- About Cryptodev
- **Current status**
- Future features
- Hardware based Virtualization
- Performance in SRIOV mode
- Summary

Supported algorithms in Cryptodev

DPDK

CIPHER ALGORITHMS

AES CBC/CTR 128/192/256 bit, Snow3G (UEA2), KASUMI F8 , NULL**

HASH ALGORITHMS

MD5_HMAC/SHA1/224*/256/384*/512, AES XCBC, Snow3G UIA2, KASUMI F9*, NULL**

AEAD ALGORITHMS

*AES GCM 128/192**/256** bit*

*Software Only,
**Hardware Only

Agenda

- About Cryptodev
- Current status
- **Planned features**
- Hardware Based Virtualization
- Performance in SRIOV mode
- Summary

Planned features in future releases

DPDK

Performance

QAT* PMD optimizations

SW PMD optimizations

Refactoring & Clean up

Algorithm support

QAT* PMD

KASUMI (F8/F9)
AES-GMAC
MD5-HMAC
SHA224/384_HMAC
NULL, 3DES-CBC

SW PMD

ZUC
3DES-CBC,
MD5
SHA1/224/256/384/512
AES-GMAC

Scheduler

Multi op scheduler with ordering maintained

Allows using hardware and software acceleration together

*QAT = Intel(R) QuickAssist Technology

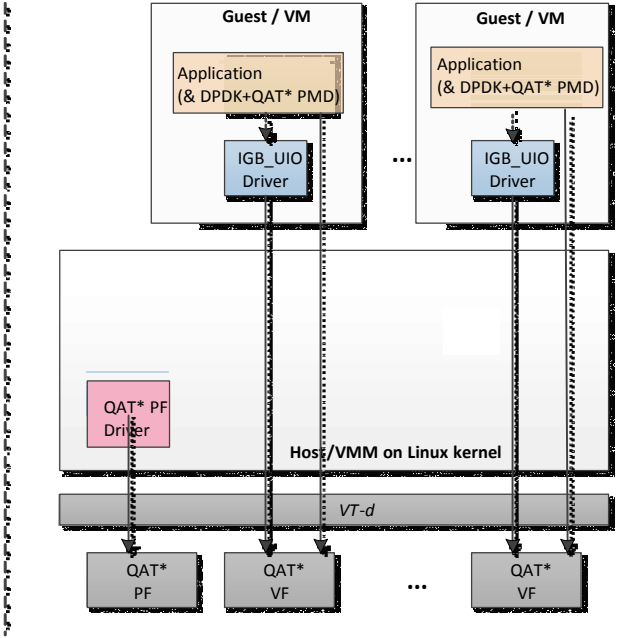
Agenda

- About Cryptodev
- Current status
- Planned features
- **Hardware Based Virtualization**
- Performance in SRIOV mode
- Summary

Hardware Based Virtualization

DPDK

- PF driver
  - Typically runs in VMM/host
  - Manages resources common to all VFs, e.g. firmware download, arbiter config, handling device/PCIe errors, etc.
- VF PMD
  - Typically runs in VM/guest, but can also be run in the VMM/host
  - Manages resources specific to the VF



Hardware-Based Virtualization SR-IOV

* QAT = Intel(R) QuickAssist Technology

Agenda

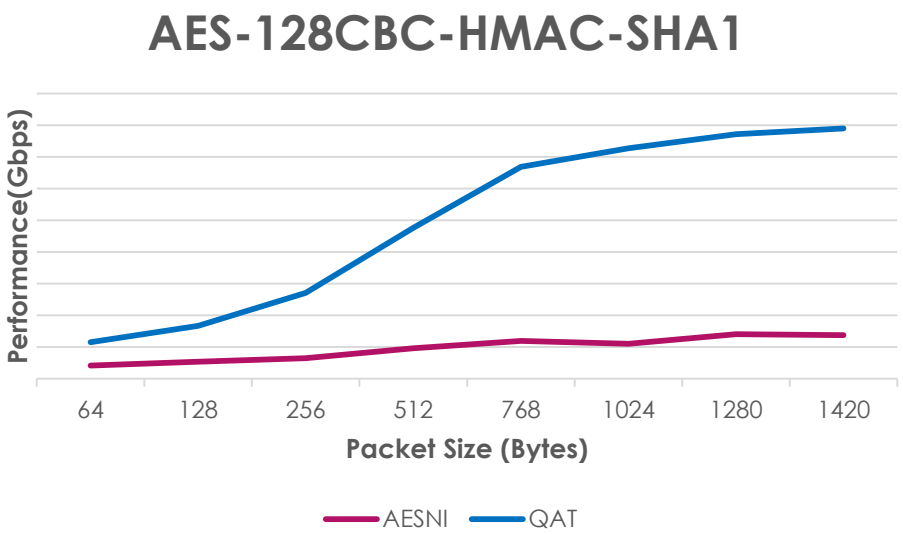
- About Cryptodev
- Current status
- Planned features
- Hardware Based Virtualization
- **Performance in SRIOV mode**
- Summary

Performance

- **SW PMD**
  - Intel® **Performance** Libraries for **AESNI, SNOW3G, KASUMI** can be used for performance boost.
- **QAT PMD in virtualized environment**
  - **Throughput** largely remains same when compared to non virtualized environment
  - **Offload Cost** also remains largely the same
  - Main difference is address translation, which is done in hardware (**VT-d IOMMU**)
  - Can add some latency depending on rate of IOTLB cache hits/misses, which can impact throughput

Performance§ from DPDK IPSec sample application

DPDK



*QAT = Intel(R) QuickAssist Technology

Intel® QuickAssist Technology

§ Mileage may vary Disclaimer: 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
Test and System Configurations: Estimates are based on internal Intel analysis using at least Data Plane Development Kit IPSec sample application on Intel(R) Xeon(R) CPU E5-2658 v4@ 2.30GHz with atleast using Intel(R) Communications Chipset(s) 8955 with Intel(R) QuickAssist Technology.

Agenda

- About Cryptodev
- Current status
- Planned features
- Hardware Based Virtualization
- Performance in SRIOV mode
- **Summary**

Summary

- Cryptodev currently provides support of symmetric algorithms.
- Provides both SW and Hardware(Intel® QuickAssist Technology) implementation.
- Healthy pipeline of features planned for Future release
- HW provides provides major boost in performance over SW implementation

Questions?

DEEPAK KUMAR JAIN

deepak.k.jain@intel.com