Compression and Security Coprocessor

XR9240

High Performance Scalable Solutions for Data Analytics, Storage, and Networking

Product Overview

Exar's XR9240 Compression and Security Coprocessor delivers unprecedented performance to OEMs in the data analytics, storage, and cloud security markets. The XR9200 family provides up to 40 gigabits/sec of simultaneous compression, encryption, and hashing while supporting up to 40,000 operations/sec of RSA (2048-bit key size). Key to the XR9240 value proposition is the ability to provide best-in-class compression ratios at maximum throughput, delivering compression ratios that are comparable with gzip level 9 while sustaining the full 40 gigabits/sec of device throughput.

Integrating an 8-lane PCI Express 3.0 host interface, the XR9240 offloads the host from CPU-intensive compression, encryption, and public key algorithms, providing the processing power of hundreds of enterprise class x86 CPU cores at much lower power and cost. In addition to the PCIe interface, the XR9240 includes a 40 gigabit/sec Interlaken interface which can optionally connect to an FPGA to provide added flexibility, enabling OEMs to enhance and differentiate their solutions with custom features. The XR9240 Class of Service provides multiple command queues to prioritize traffic, avoiding over provisioning and enforcing service level agreements for performance critical applications. The XR9240 incorporates Single Root I/O Virtualization (SRIOV) to support virtualized environments, integrating 128 virtual functions.

The XR9240 includes a user friendly Software Development Kit (SDK) which includes a wide range of features for enhanced performance, advanced management and monitoring, and high reliability and availability. The SDK is API-compatible with the 8200 family of coprocessors.

Key Benefits

The XR9240 leading edge compression engine minimizes the data footprint while maximizing performance, delivering a multitude of benefits. Costly I/O bottlenecks for both storage and networking are removed or minimized, enabling maximum system throughput at minimum latency.

Storage and data analytics applications benefit from higher bandwidth disk I/O and higher storage capacity. Data encryption and hashing are also supported in addition to compression without suffering penalties in either performance or latency.

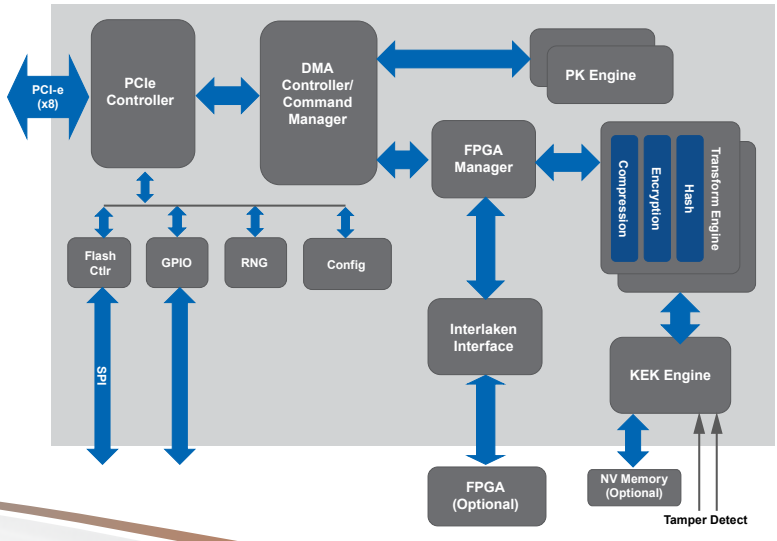
The XR9240 supports a wide range of encryption, authentication, and public key algorithms for networking security, providing all required support for IPsec and SSL/TLS/DTLS, including high performance public key processing, which enables the secure infrastructure needed to support the high transaction throughput required by cloud and web-based applications. Security features also include support for the elliptic curve cryptography (ECC) algorithms and Suite B.

The XR9240's pipelined hardware state machine architecture allows compression, encryption, hashing, and PK engines to run at maximum performance simultaneously, removing the need for device partitioning and providing deterministic performance and latency for enterprise applications.

Target Applications

The XR9240's high performance, scalability, and low power address the requirements for a variety of enterprise applications, including data warehouses, Hadoop clusters, storage arrays, application delivery controllers, WAN optimization appliances, security gateways, and hardware security modules.

XR9240 Block Diagram



Compression and Security Coprocessor

XR9240

High Performance Scalable Solutions for Data Analytics, Storage, and Networking

Feature Summary

Category	Key Features
Compression	• gzip, zlib, Deflate, eLZS, LZS
Encryption/ Decryption	• AES (128, 192, 256): CBC, GCM, CTR, ECB, F8 • 3DES, DES, ARC4
Hashing	• MD5, SHA-1, SHA-2 (224, 256, 384, 512)
Authentication	• HMAC-MD5, HMAC-SHA-1, HMAC-SHA-2 (224, 256, 384, 512), GMAC (AES), XCBC MAC, CMAC, SSL 3.0 MAC
Public Key	• RSA and DH (up to 4K bits), DSA • ECDH and ECDSA (P-192 to P-521)
Randon Number Generation	• Hardware RNG • SP800-90 DRBG
Suite B	• Top Secret and Secret
Virtualization	• Up to 128 Virtual Functions

Category	Key Features
Class of Service	• 8 Class Queues for Comp/Encr/Hash • 4 Class Queues for PK operations
Customization	• Optional FPGA connected to Interlaken interface enables custom features
Key Encryption Key (KEK)	• Key unwrap engine, KEK store, tamper detection
Reliability	• Automatic failover upon error detection • Real time transform verification
Host Interface	• PCIe 3.0 (x8)
Expansion Interface	• Interlaken (x8) • 3.125 or 6.25 Gbit/sec per lane
Power Efficiency	• Fine grained power management • Dynamic clock gating
Package	• 31 x 31 mm FCBGA
Operating System Support	• RHEL 6, SLES 11, Ubuntu 14, FreeBSD 9
System Software Support	• AltraHD, OpenSSL

DX9240 Summary

Product	Maximum Performance CompressionEncryption/Hash	Maximum Performance RSA 2048-bit ops/sec	Power Consumption* (typ)
XR9240	40 Gbit/sec/ 5 GB/sec	40K	14.6W

* Total device power includes compression, encryption, hashing, PK, Interlaken

EXAR CORPORATION
48720 Kato Road
Fremont, CA 94538
U.S.A.
T. +1.510.668.7000
F. +1.510.668.7001

FLY0814_XR9240

www.exar.com