Acceleration Card

Express DX 1700 Series

Data Reduction and Security Solutions for the Unified Storage and Network Infrastructure

The massive amount of digital content and its global distribution is not only straining the compute, storage and networking infrastructure of large Enterprises and SMBs but also plaguing the cost-sensitive consumer and SOHO market segments.

Fortune 500 companies and SMBs are struggling to manage the exponential growth in data, its mobility and supporting a dynamic virtualized IT infrastructure required to address an increasingly demanding business environment. However, the vast majority of IT budgets are spent maintaining the existing storage and network infrastructure. Power, cooling, real estate, and the ever-increasing demand for compute, storage, network and application resources all continue to push costs higher.

Furthermore the growth in global online transactions and content distribution across heterogeneous networks as well as storing information on mobile or removable media is raising security concerns. Customers across the board want to ensure that their data is secure whether it is in transit across the network or at rest on their storage devices.

DX 1700 Series Solutions

The DX 1700 series cards offload the computationally intensive tasks necessary to compress, deduplicate, and secure data in both block form for storage applications and packet form for networking applications. These products are aimed at enabling a more unified and efficient compute, storage and network infrastructure for SOHO, SMB and enterprise class customers.

These cards offer power efficient hardware acceleration capabilities for data compression, deduplication, and network and storage security.

Hardware Offload

Hardware offload frees up valuable and expensive CPU resources to be utilized for improving application performance and enabling virtualized environments. Offloaded algorithms include:

* Data Reduction: eLZS, LZS and GZIP
* Security / Encryption: AES-CBC, -CTR, -GCM, -ECB; 3DES
* Security / Authentication: AES-GCM, -GMAC, -XCBC-MAC; HMAC-SHA-1, -256, -384; HMAC-MD5; SSL3.0-MAC
* Hash for Deduplication: SHA-1, -256, -384; MD5
* Public Key: RSA, DH, DSA, ECDH and ECDSA
* OpenSSL and OpenSwan (using NETKEY) support (Availability Q1CY11)
* Suite B Support

Performance and Scalability

* Throughput of up to 800 MB/sec (6.4 Gb/sec)
* Up to 14,200 Operations / sec for RSA 1K keys
* Multiple cards can be integrated into a system to attain aggregate performance
* Load balancing across multiple cards

High Availability

* End-to-end data protection assures data integrity by detecting, isolating and preventing the propagation of corrupt data caused by silent disk errors, application interaction and memory errors
* New software architecture provides failover protection in case of a card failure

Security

The cards offer a broad set of encryption algorithms enabling customers to select the desired security level for information sent over the LAN/WAN or at rest in a storage array. The flexibility to select the appropriate security level also simplifies implementation of policy based access and strengthens overall network security.

Power Efficiency

The DX 1700 series cards were designed to minimize power consumption and cooling costs. Typical power consumption ranges from 1.9 W to 3.3 W depending on performance grade.

STORAGE SYSTEM APPLICATIONS

* Consumer/SOHO Network-Attached Storage (NAS)
* Enterprise Network-Attached Storage (NAS)
* Direct-Attached Storage (DAS)
* Storage Area Network (SAN)
* Disk backup and archival servers, offering:
  – Remote Replication
  – Data deduplication
  – Continuous Data Protection (CDP)
  – Snapshot and Replication
  – Disk-to-Disk (D2D)
  – Virtual Tape Library (VTL)
  – Content-Addressable Storage (CAS)
* Tape backup servers

NETWORK APPLICATIONS

* Unified Threat Management Appliances
* Enterprise Secure Router / VPN Gateway/Wireless Backhaul
* Enterprise VPN Firewall
* Data Center Load Balancers
* Multi Service Switches
* Layer 4-7 Switches
* Wireless Base Stations
* Radio Network Controllers
* Carrier Network Security
* WAN Optimization Appliances

DX 1700 Series
Data Reduction and Security
Acceleration Cards

www.exar.com

Express DX 1700 Series

EXAR

Data Reduction and Security Solutions
for the Unified Storage and Network Infrastructure

	DX 1710 / 20/ 30 / 40
KEY FEATURES	
Data Reduction Algorithms	• eLZS, LZS, GZIP (Deflate RFC 1951)
Encryption / Decryption	• AES (128, 192, 256) CBC, GCM, CTR, ECB, XTS-256, XTS-512 • 3DES, DES, ARC4
Authentication	• AES-GMAC, -XCBC-MAC • HMAC-SHA-1, -256 , -384; HMAC-MD5 • SSL3.0-MAC
Hashing for Deduplication	• SHA-1, SHA-256, SHA-384 • MD5
Public Key	• RSA and DH up to 8k-bits, DSA • ECDH and ECDSA (256-bit, 384-bit, 521-bit)
Random Numbers	• Hardware random number generator • ANSI X9.31 PRNG
Suite B Support	Broadest set of cryptographic algorithms for government applications • Top Secret: AES-GCM-256/AES-GMAC-256, SHA-384, ECDSA-384, ECDH-384 • Secret (and below): AES-GCM-128/AES-GMAC-128, SHA-256, ECDSA-256, ECDH-256
Open Source Network Security	• OpenSSL • OpenSwan • Availability Q1CY11
Performance / Throughput	See table below
Performance Features	• Compression, hash and encryption in a single pass • Automatic load balancing • Hardware-assisted command chaining and scatter gather (unlimited buffers)
Ease of Use	• New SDK simplifies integration and reduces time to market • Intel QuickAssist API Support
Power and Space Efficiency	• Fine grain power management ensures lowest real-time power consumption per command
Reliability and Service Features	• Software failover protection (All HW functionality) in case of card failure • End-to-end data integrity (On chip and off chip error detection) • Complete verification of compressed, encrypted and hash data in real time with no performance impact

	DX 1710 / 20/ 30 / 40
CARD SPECIFICATIONS	
Bus Interface	• PCIe x1, x4 • PCIe Spec. Rev. 2.0 compliant, Gen 1 speed (2.5 Gbps)
Card Dimensions	• Length: 9.08 cm (3.58 in) • Height: 6.89 cm (2.71 inches)
Bracket Dimensions	Low profile: 1.84 x 7.92 cm (0.73 x 3.12 in) Optional full height: 1.84 x 12.00 cm (0.73 x 4.73 in)
ENVIRONMENTAL SPECIFICATIONS	
Temperature and Humidity	Operating: 0°C/32°F to 55°C/131°F; 10% to 90% RH non-condensing Storage: -10°C/14°F to 70°C/158°F; 5% to 95% RH non-condensing
Required Airflow	None (@ 55°C operating, sea level)
Material Safety	RoHS-6
AGENCY APPROVALS	
Safety	USA: UL60950-1, 2nd Edition European Community: EN 60950-1, Low voltage directive 2006/95/EC and EMC directive 2004/108/EC Canada: cUL CSA C22.2 No. 60950-1-03
EMI and EMC	USA: FCC Part 15, Class B Canada: ICES-003[B], NMB-003[B] European Community: EN55022:2006, EN55024:1998 Japan: VCCI V-3/2008.04, Class B Taiwan: BSMI CNS13438:95(2006) Class B New Zealand/Australia: AS/NZS CISPR22 Korea: KCC KN22/KN24
SDK AND OS SUPPORT	
SDK Features	• Raw Acceleration API for Networking Applications • Data Offload API for Storage Applications • QuickAssist API (Intel standard) • Functional example applications show API usage • Demo application for testing performance • OS Abstraction Layer allows easy porting to custom OS
Operating Systems Supported	• Windows Server 2003 R2 (32/64 bit) • Windows Server 2008 R2 (32/64 bit) • Red Hat Enterprise Linux 4 Update 6 (32/64 bit) • Red Hat Enterprise Linux 5 & Update 1 (32/64 bit) • Novell SUSE ELS 9 SP 4 (32/64 bit) • Novell SUSE ELS 10 (32/64 bit)

Product Selector Guide

PRODUCT	PERFORMANCE (Refer to Note 2)			COMPRESSION			ENCRYPTION			HASH			PACKET PROCESSING ACCELERATION	POWER		PCIe CARD (HALF HEIGHT/ HALF LENGTH)
Model no.	Mbps	MB/s	1k RSA, Ops/s	LZS	eLZS	GZIP	AES	DES, 3DES	ARC4	SHA-1, MD5	SHA-256, SHA-384 (Note 3)	True Rng	IPsec, IPComp SSL/TLS	Typ (W)	Max (W)	Interface
DX 1740	6,400	800	14,200	√	√	√	√	√	√	√	√	√	√ (Note 1)	3.3	5.5	PCIe x4
DX 1730	3,200	400	7,100	√	√	√	√	√	√	√	√	√	√ (Note 1)	2.5	4.5	PCIe x4
DX 1720	1,600	200	3,550	√	√	√	√	√	√	√	√	√	√ (Note 1)	2.0	4.0	PCIe x4
DX 1710	800	100	1,775	√	√	√	√	√	√	√	√	√	√ (Note 1)	1.9	3.8	PCIe x1

Note 1: Raw crypto/compression performed on-chip; packet header/trailer manipulation performed in software at application level
Note 2: Refer to performance application note for specific performance results for each algorithm.
Note 3: SHA-384, HMAC-SHA-384 supported in software.

www.exar.com