

# NITROX™ *Lite* Security Macro Processor

## SSL Family Product Brief

### PRODUCT FEATURES & BENEFITS

#### Worlds first Security Macro Processor developed using custom CPU design techniques

- Single chip solution that accelerates all cryptographic operations and the complete SSL protocol

#### High performance Public Key Processor

- 500 to 7K 1024bit RSA operations/second
- 500 to 12K 1024bit Diffie Hellman ops/sec
- Up to 4K full SSL or TLS Handshakes/sec (TPS)

#### High performance Bulk Data Encryption

- 50 Mbs to 1000 Mbps Record Processing (Bulk Data Encryption + Hashing)

#### Multi Algorithm Support

- RSA and Diffie-Hellman
- DES/3DES, AES, ARC4
- MD5, SHA-1, HMAC-MD5, HMAC-SHA-1

#### High number of concurrent SSL sessions supported

- Supports unlimited SSL sessions with host memory

#### On Chip True Random Number Generator

#### High performance native Interfaces

- PCI-X (64bit, 133 MHz, Master and Slave modes)
- PCI (32bit, 66MHz, Master and Slave modes)
- PCI (64bit, 66MHz, Master and Slave modes)

128 LQFP(32bit PCI only) or 256 BGA

Typical Power 1.0W

Industrial temp version available

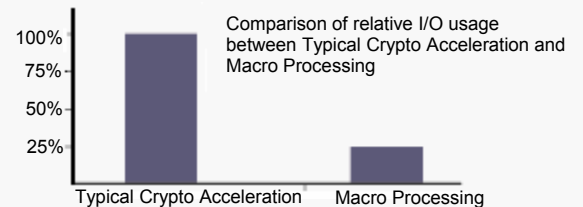
### PROTOCOL & MANAGEMENT SUPPORT

#### Multi Protocol Support

- Macro support for SSL, TLS and WTLS

#### Full SSL Protocol Processing with specialized TurboSSL Macro API functions

- Macro API functions result in dramatic reduction of required I/O bus bandwidth



#### Adapts to handle various bandwidth requirements of different cryptographic operations

- Truly balanced systems can be designed using NITROX *Lite* that can adapt to various SSL handshakes/sec and SSL record processing loads based on website demand

#### Dedicated Resources for Administration & Management

- Extensive functionality to assist a range of functions including, statistics collection, logging, etc.

#### Software drivers for popular operating systems such as Linux, BSD and Windows

#### Modified OpenSSL with Cavium's TurboSSL Macro API calls

Figure 1: Example of NITROX *Lite* as an SSL accelerator

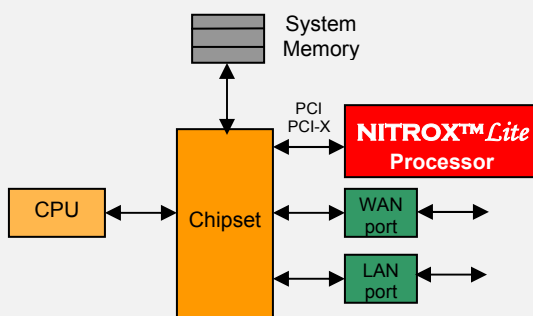
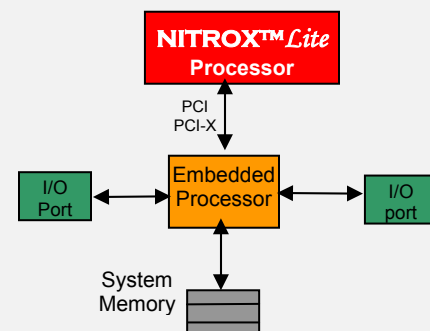


Figure 2: Example of NITROX *Lite* in embedded system as an SSL accelerator



## APPLICATIONS

### Servers

- SSL acceleration for Web Servers - Microsoft IIS and Linux Apache
- Ideal for 1-2 processor servers

### Web Appliances

- SSL Proxy Server, SSL based VPNs
- Servers hosting SSL based remote access for secure email and other enterprise applications

### Wireless WAP gateways

## BENEFITS TO DESIGNERS

### Reduced system cost and complexity

- Single custom processor solution

### Quick time to market with complete

- Evaluation board, processor, software
- Software driver and application

### Flexible Protocol Processing

- Flexible microcode allows for advanced processing with field upgrade option

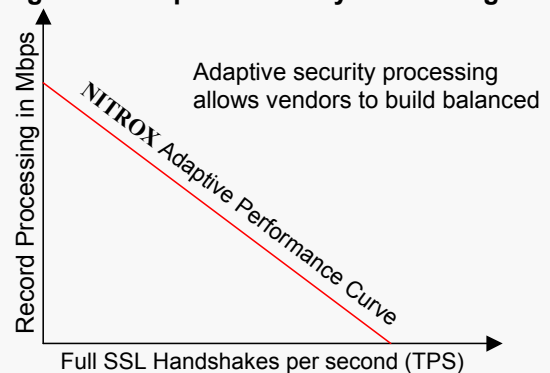
## PRODUCT SUMMARY

The NITROX *Lite* Macro Security Processor is the industry's first processor exclusively targeted towards high performance SSL applications as opposed to plain cipher acceleration. The NITROX *Lite* custom designed processor provides lowest area, cost and power consumption when compared to ASIC based security chips. The heart of NITROX *Lite* is the micro-programmed GigaCipher core, which allows for future upgrades and flexibility in supporting all cryptographic operations and protocol layer functions.

Figure 3 shows how multiple cores provide adaptive processing power that can be used for all cryptographic operations and protocol processing. This feature is unique to the NITROX *Lite* and allows for flexible response to dynamic load. For example, an e-commerce website requires a large ratio of SSL handshakes/sec vs SSL record processing when compared to an online stock brokerage website that requires more SSL record processing vs SSL handshakes/sec. This adaptive nature of NITROX *Lite* allows vendors to build balanced systems that can handle dynamic traffic conditions.

NITROX *Lite* is the only processor that has the capability to process high-level SSL protocol macro commands that reduce the host I/O traffic and dramatically offload the system processor to increase the total system throughput. The NITROX *Lite* SDK includes an evaluation board with modified OpenSSL using Cavium's TurboSSL Macro APIs and software drivers for popular operating systems such as Linux, BSD and Windows.

Figure 3: Adaptive Security Processing



## Ordering Information

Part Number	Bus	Maximum RSA 1024bit	Maximum ARC4+SHA-1	Package
CN501-183LQ128	PCI 32-bit, 33 or 66MHz	900	100	128 LQFP
CN505-183LQ128	PCI 32-bit, 33 or 66MHz	1750	200	128 LQFP
CN1001-350BG256	PCI 32bit / 66MHz	1750	200	256 BGA
CN1005-350BG256	PCI 64bit / 66MHz	3500	400	
CN1010-350BG256	PCI-X 64bit/133 MHz	7000	1G	

For PCI-X parts for CN1001, CN1005 and CN1010 add -X at the end