Fact Sheet

MPC190

SECURITY PROCESSOR

Network equipment vendors looking to integrate the latest security systems into their equipment can now turn to Motorola—the same company that makes the network and communications processors the industry knows and trusts. Derived from 30 years of security technology experience, Motorola's family of network security processors is designed to work seamlessly with Motorola's communications processors and offers an easy way to enhance the performance of network equipment without adding costly hardware.

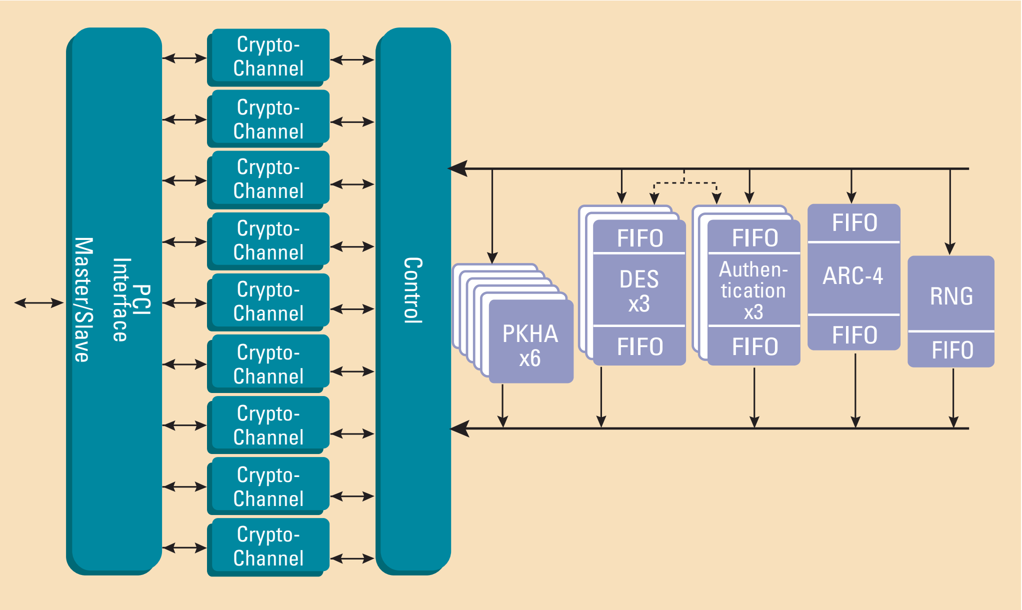
The MPC190 security processor is a powerful addition to any networking or computing system supporting the widely used PCI interface standard. It is designed to off-load computationally intensive security functions, such as key generation and exchange, authentication, and bulk encryption from Motorola's processors, including the PowerQUICC II™ communications processors with integrated PCI, MPC8265, MPC8266, or from any processor through the use of a PCI bridge chip.

The MPC190 security processor is optimized to process all the algorithms associated with IPsec, IKE, WTLS/WAP and SSL/TLS, including RSA, RSA signature, Diffie-Hellman, Elliptic Curve Cryptography, DES, 3DES, SHA-1, MD-4, MD-5, and ARC-4. The MPC190 is also capable of accelerating Elliptic Curve mathematics, which is especially important for secure wireless communications.

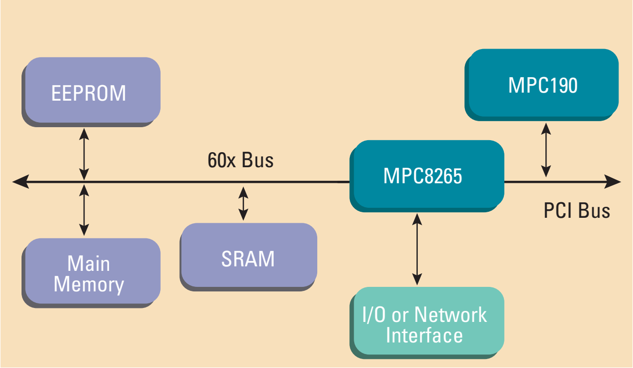
MPC190 PRODUCT HIGHLIGHTS:

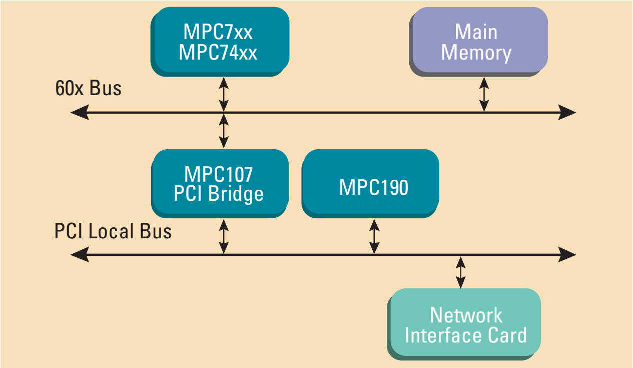
- Six Public Key Execution Units (PKEUs) that support the following:
- RSA and Diffie-Hellman
  - Programmable field size 80- to 2048-bits
  - Elliptic curve operations in either F2m or F(p)
  - Programmable field size from 55 to 511 bits
- Three Data Encryption Standard Execution Units (DEUs)
  - DES
  - 3DES
  - Two key (K1, K2, K1) or Three key (K1, K2, K3)
  - ECB and CBC modes for both DES and 3DES
- ARC Four Execution Unit (AFEU)
  - Implements a stream cipher compatible with the RC4 algorithm
  - 40- to 128-bit programmable key

MPC190 BLOCK DIAGRAM



MPC190 CONNECTED TO POWERQUICC II™ PCI BUS





MPC190 CONNECTED TO MOTOROLA HOST PROCESSOR CPU VIA BRIDGE

- Three Message Digest Execution Units (MDEUs)
  - SHA-1 with 160-bit message digest
  - MD4 or MD5 with 128-bit message digest
  - HMAC with either algorithm
- Random Number Generator (RNG)
- PCI 2.2-compliant external bus interface, with master/slave logic.
  - 32-bit address/64-bit data, 66 MHz
  - 32-bit address/32-bit data mode
- Nine crypto-channels, each supporting multi-command descriptor chains
  - Static and/or dynamic assignment of crypto-execution units via an integrated controller
  - Buffer size of 2 KB for each crypto-channel
- 1.8V supply, 3.3V I/O
- 252 MAP BGA
- 2.0W power dissipation
- Software and development support available

TYPICAL APPLICATIONS:

- Edge routers
- DSLAMS
- Broadband access equipment
- e-Commerce servers
- Wireless base stations
- WAP gateways

MPC190 PERFORMANCE:

- 1024-bit Diffie-Hellman
  -520 connections per second
- 155-bit ECC
  -1000 connections per second
- DES 1.13 Gbps
- 3DES 0.68 Gbps
- MD5 0.97 Gbps
- 3DES-HMAC-SHA-1 0.60 Gbps

Bulk encryption/authentication performance estimates include data/key/context reads from memory to MPC190, writes of completed data/context to memory by MPC190 assuming typical PCI system overhead. The MPC190 supports single pass processing of encryption/message authentication.

MOTOROLA

The MPC190 security processor contains a PowerPC processor core.