Fact Sheet

MPC184

SECURITY PROCESSOR

MOTOROLA intelligence everywhere™ | digital dna™

Network equipment vendors looking to integrate the latest security standards 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.

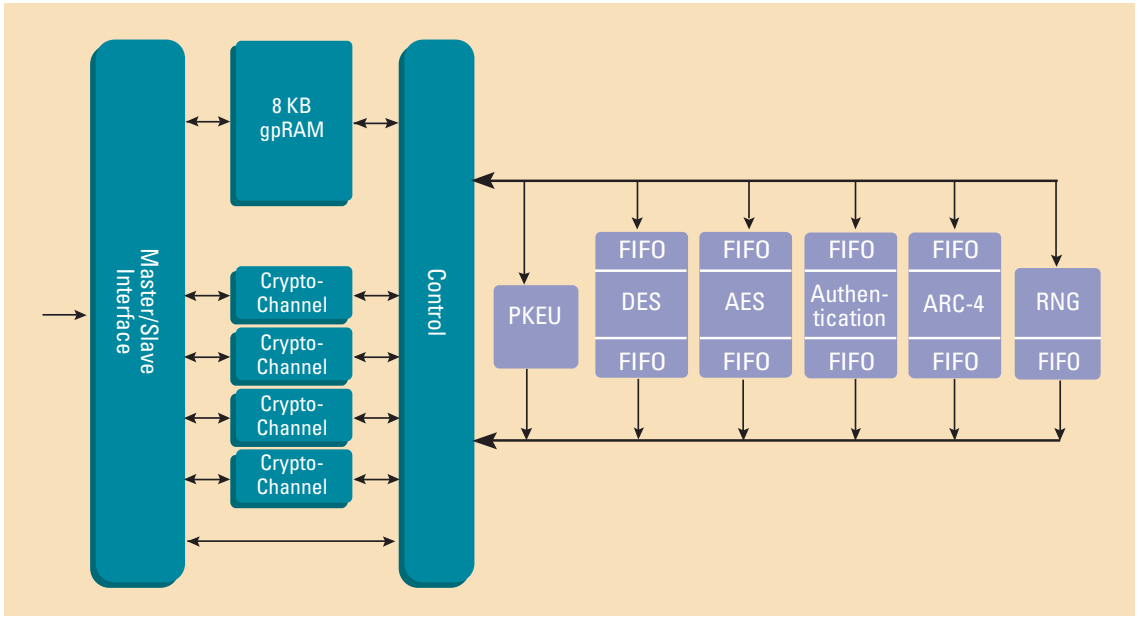
The MPC184 security processor is optimized for any system supporting Motorola's 8xx bus and the 32-bit PCI interface standard. It is designed to off-load computationally intensive security functions, such as key generation and exchange, authentication, and bulk encryption from processors such as Motorola's MPC8xx and MPC824x family of integrated host processors, or from any processor through the use of a PCI bridge chip.

The MPC184 security processor is optimized to process the algorithms associated with IPsec, IKE, WTLS/WAP and SSL/TLS, including RSA, RSA signature, Diffie-Hellman, Elliptic Curve Cryptography, DES, 3DES, AES, SHA-1, SHA-256, MD-5, and ARC-4. The MPC184 is one of Motorola's first security processors to support the newly adopted AES standard.

MPC184 PRODUCT HIGHLIGHTS:

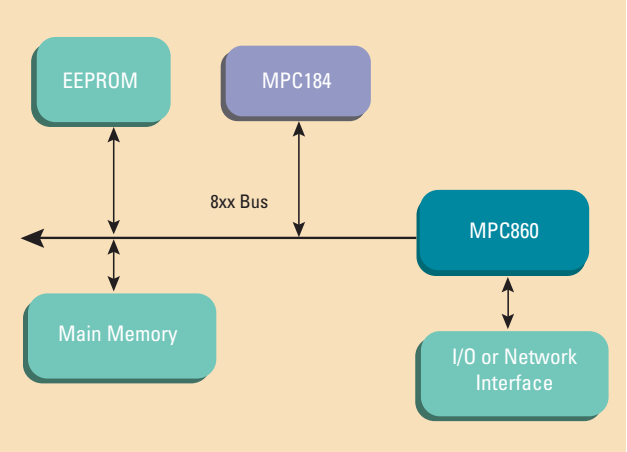
- One Public Key Execution Unit (PKEU) that supports the following:
  - RSA and Diffie-Hellman
  - Programmable field size up to 2048 bits
  - Elliptic curve cryptography
  - F2m and F(p) modes
  - Programmable field size up to 511 bits
- One Data Encryption Standard Execution Unit (DEU)
  - DES, 3DES
  - Two key (K1, K2, K1) or three key (K1, K2, K3)
  - ECB and CBC modes for both DES and 3DES

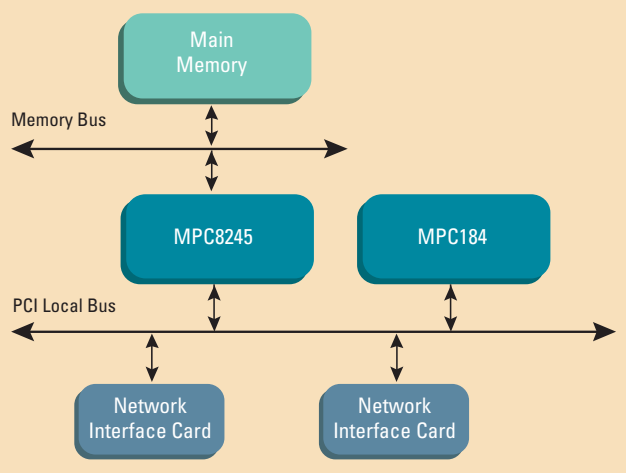
MPC184 BLOCK DIAGRAM



- One Advanced Encryption Standard Unit (AESU)
  - Programmable key length of 128, 192, or 256 bits
  - Implements the Rinjdael symmetric key cipher
- One ARC Four Execution Unit (AFEU)
  - Implements a stream cipher compatible with the RC4 algorithm
  - 40- to 128-bit programmable key
- One Message Digest Execution Unit (MDEU)
  - SHA-1 with 160-bit message digest or SHA-2 with 256-bit message digest
  - MD5 with 128-bit message digest
  - HMAC with any algorithm
- One Random Number Generator (RNG)
- 8xx-compliant external bus interface, with master/slave logic
  - 32-bit address/32-bit data
  - Up to 66 MHz operation
- PCI 2.2-compliant external bus interface, with master/slave logic
  - 32-bit address/32-bit data mode, 66 MHz
- Four crypto-channels, each supporting multi-command descriptor chains
  - Static and/or dynamic assignment of crypto-execution units via an integrated controller
  - Buffer size of 512 bytes for each execution unit, with flow control for large data sizes
- 8 KB of internal scratchpad memory for key, IV and context storage
- 1.5V supply, 3.3V I/O
- 252 MAP BGA
- 1.0W power dissipation
- Software and development support available

MPC184 CONNECTED TO POWERQUICC II™ 8XX BUS





MPC184 CONNECTED TO AN INTEGRATED HOST PROCESSOR SUCH AS THE MPC8245

TYPICAL APPLICATIONS:

- SOHO/ROBO routers
- DSLAMS
- Broadband access equipment
- e-Commerce servers
- WAP gateways

MPC184 PERFORMANCE:

- 1024-bit Diffie-Hellman
  - 60 connections per second
- 155-bit ECC
  - 100 connections per second
- DES 247 Mbps
- 3DES 144 Mbps
- MD5 176 Mbps
- SHA-1 144 Mbps
- 3DES-HMAC-SHA-1 123 Mbps
- AES-128 124 Mbps
- AES-256 105 Mbps

Bulk encryption/authentication performance estimates are based on large packets, and include data/key/context reads from memory to MPC184, writes of completed data/context to memory by MPC184, assuming typical system overhead. The MPC184 supports single pass processing of encryption/message authentication.

MOTOROLA

The MPC184 security processor contains a PowerPC processor core.

MPC184FACT/D
REV 1

Freescale Semiconductor, Inc.