Chipsmall Limited consists of a professional team with an average of over 10 year of expertise in the distribution of electronic components. Based in Hongkong, we have already established firm and mutual-benefit business relationships with customers from,Europe,America and south Asia,supplying obsolete and hard-to-find components to meet their specific needs.

With the principle of “Quality Parts,Customers Priority,Honest Operation,and Considerate Service”,our business mainly focus on the distribution of electronic components. Line cards we deal with include Microchip,ALPS,ROHM,Xilinx,Pulse,ON,Everlight and Freescale. Main products comprise IC,Modules,Potentiometer,IC Socket,Relay,Connector.Our parts cover such applications as commercial,industrial, and automotives areas.

We are looking forward to setting up business relationship with you and hope to provide you with the best service and solution. Let us make a better world for our industry!

Contact us

Tel: +86-755-8981 8866 Fax: +86-755-8427 6832
Email & Skype: info@chipsmall.com Web: www.chipsmall.com
Address: A1208, Overseas Decoration Building, #122 Zhenhua RD., Futian, Shenzhen, China

MPC180LMB Security Processor User's Manual

Rev. 1, 3/2002

Digital DNA from Motorola

MOTOROLA

DigitalDNA, PowerQUICC, and PowerQUICC II are trademarks of Motorola, Inc.

The PowerPC name, the PowerPC logotype, and PowerPC 603e are trademarks of International Business Machines Corporation used by Motorola under license from International Business Machines Corporation.
I^2C is a registered trademark of Philips Semiconductors

This document contains information on a new product under development. Motorola reserves the right to change or discontinue this product without notice. Information in this document is provided solely to enable system and software implementers to use Motorola security processors. There are no express or implied copyright licenses granted hereunder to design or fabricate Motorola security processors integrated circuits or integrated circuits based on the information in this document.

Motorola reserves the right to make changes without further notice to any products herein. Motorola makes no warranty, representation or guarantee regarding the suitability of its products for any particular purpose, nor does Motorola assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. “Typical” parameters can and do vary in different applications. All operating parameters, including “Typicals” must be validated for each customer application by customer’s technical experts. Motorola does not convey any license under its patent rights nor the rights of others. Motorola products are not designed, intended, or authorized for use as components in systems intended for surgical implant into the body, or other applications intended to support or sustain life, or for any other application in which the failure of the Motorola product could create a situation where personal injury or death may occur. Should Buyer purchase or use Motorola products for any such unintended or unauthorized application, Buyer shall indemnify and hold Motorola and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that Motorola was negligent regarding the design or manufacture of the part. Motorola and Ⓜ are registered trademarks of Motorola, Inc. Motorola, Inc. is an Equal Opportunity/Affirmative Action Employer.

Motorola Literature Distribution Centers:

USA/EUROPE: Motorola Literature Distribution; P.O. Box 5405; Denver, Colorado 80217; Tel.: 1-800-441-2447 or 1-303-675-2140/

JAPAN: Nippon Motorola Ltd SPD, Strategic Planning Office 4-32-1, Nishi-Gotanda Shinagawa-ku, Tokyo 141, Japan Tel.: 81-3-5487-8488

ASIA/PACIFC: Motorola Semiconductors H.K. Ltd.; 8B Tai Ping Industrial Park, 51 Ting Kok Road, Tai Po, N.T., Hong Kong; Tel.: 852-26629298

Technical Information: Motorola Inc. SPS Customer Support Center 1-800-521-6274; electronic mail address: crc@wmkmail.sps.mot.com.

Document Comments: FAX (512) 933-3873, Attn: Security Processor Applications Engineering.

World Wide Web Addresses: http://www.motorola.com/smartnetworks/products/security
http://www.mot.com/netcomm
http://www.mot.com/PowerPC
http://www.mot.com/HPESD

CONTENTS

CONTENTS

CONTENTS

Chapter 8
Random Number Generator

CONTENTS

ILLUSTRATIONS

ILLUSTRATIONS

TABLES

TABLES

Chapter 1
Overview

This chapter gives an overview of the MPC180 security processor, including the key features, typical system architecture, and the MPC180 internal architecture.

1.1 Features

The MPC180 is a flexible and powerful addition to any networking system currently using Motorola's MPC8xx or MPC826x family of PowerQUICC™ communication processors. The MPC180 is designed to off-load computationally intensive security functions such as key generation and exchange, authentication, and bulk data encryption.

The MPC180 is optimized to process all of the algorithms associated with IPSec, IKE, WTLS/WAP and SSL/TLS. In addition, the MPC180 is the only security processor on the market capable of executing the elliptic curve cryptography that is especially important for secure wireless communications.

MPC180 features include the following:

- Public key execution unit (PKEU), which supports the following:
  - RSA and Diffie-Hellman
    - Programmable field size 80- to 2048-bits
    - 1024-bit signature time of 32ms
    - 10 IKE handshakes/second
  - Elliptic Curve operations in either F 2 m or F p
    - Programmable field size from 55- to 511-bits
    - 155-bit signature time of 11ms
    - 30 IKE handshakes/second
- Message authentication unit (MAU)
  - SHA-1 with 160-bit message digest
  - MD5 with 128-bit message digest
  - HMAC with either algorithm
- Data encryption standard execution units (DEUs)
  - DES and 3DES algorithm acceleration
    - Two key (K1, K2, K1) or Three key (K1, K2, K3)

  - — ECB and CBC modes for both DES and 3DES
  - — 15 Mbps 3DES-HMAC-SHA-1 (memory to memory)
- ARC four execution unit (AFEU)
  - — Implements a stream cipher compatible with the RC4 algorithm
  - — 40- to 128-bit programmable key
  - — 20 Mbps ARC Four performance (memory to memory)
- Random Number Generator (RNG)
  - — Supplies up to 160 bit strings at up to 5 Mbps data rate
- Input Buffer (4kbits)
- Output Buffer (4kbits)
- Glueless interface to MPC8xx system or MPC826x local bus (50MHz and 66MHz operation)
- DMA hardware handshaking signals for use with the MPC826x
- 1.8v Vdd, 3.3v I/O
- 100pin LQFP package
- HIP4 0.25µm process

1.2 System Architecture

The MPC180 works well in most load/store, memory-mapped systems. An external processor may execute application code from its ROM and RAM, using RAM and optional non-volatile memory (such as EEPROM) for data storage. Figure 1-1 shows an example of the MPC180 in an MPC8xx system, and Figure 1-2 shows the MPC180 connected to the local bus of the MPC826x. In these examples, the MPC180 resides in the memory map of the processor; therefore, when an application requires cryptographic functions, it reads and writes to the appropriate memory location in the security processor.

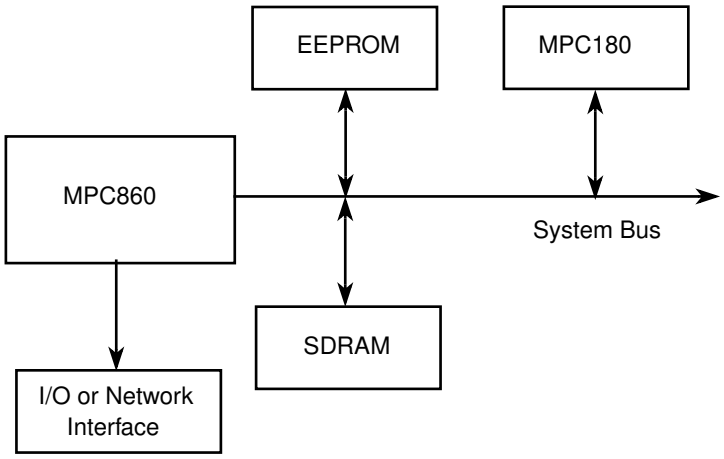

Figure 1-1. Typical MPC8xx System Example

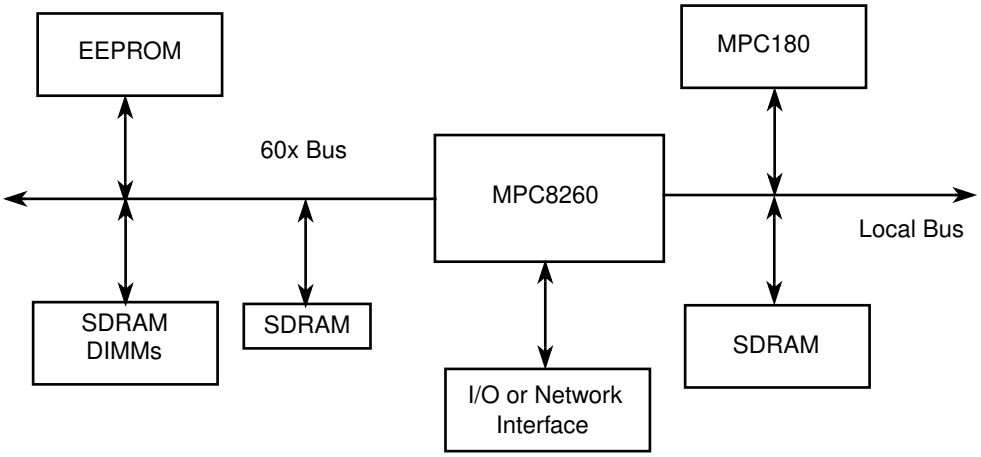

Figure 1-2. Typical MPC8260 System Example

1.3 Architectural Overview

The MPC180 has a slave interface to the MPC8xx system bus and MPC8260 local bus and maps into the host processor's memory space. Each encryption algorithm is mapped to a unique address space. To perform encryption operations, the host reads and writes to the MPC180 to setup the execution unit and, then, transfers data to the execution unit directly or through the external bus interface.

In FIFO mode, the MPC180 accepts data into the 4-Kbit input buffer and returns burst data through the output buffer. In this way, the host can automatically transfer bulk data through a given EU. This minimizes host management overhead and increases overall system throughput. Once the host configures the external bus interface (EBI), it receives an interrupt only after all data has been transferred or processed by the MPC180.

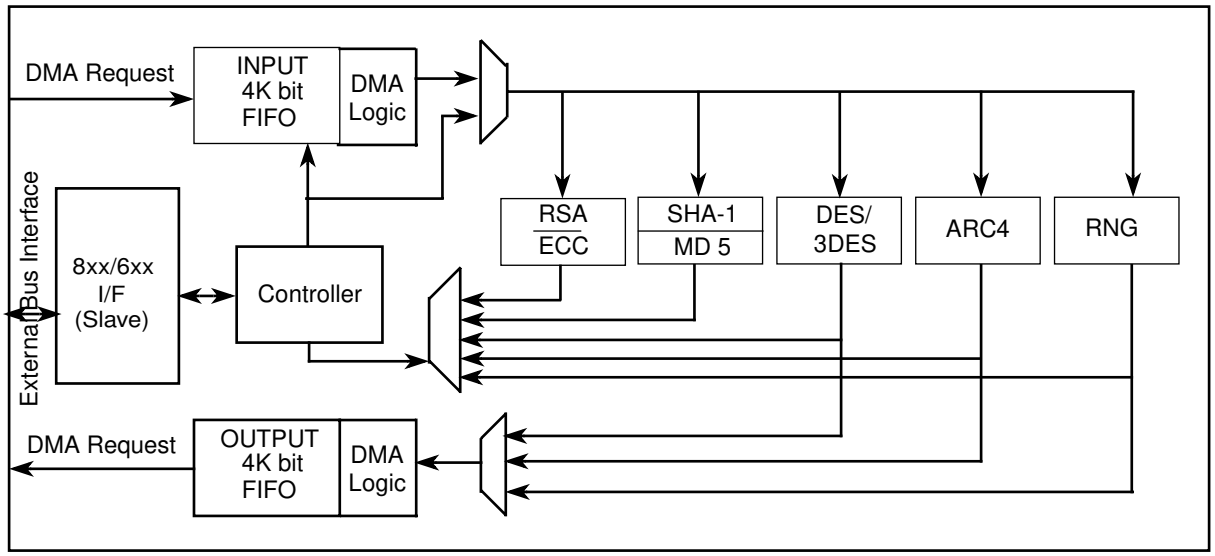

Figure 1-3. MPC180 Block Diagram

The interrupt controller organizes hardware interrupts coming from individual EUs into a single maskable interrupt, IRQ_B, for the host processor. Multiple internal interrupt sources are logically ORed to create a single, non-prioritized interrupt for the host processor. The controller lets the host read the unmasked interrupt source status as well as the request status of masked interrupt sources, thereby indicating whether a given unmasked interrupt source will generate an interrupt request to the host processor.

1.3.1 Public Key Execution Unit (PKEU)

The PKEU is capable of performing many advanced mathematical functions to support RSA and Diffie-Hellman as well as ECC in both F 2 m (polynomial-basis) and F p. The accelerator supports all levels of functions to assist the host microprocessor in performing its desired cryptographic function. For example, at the highest level, the accelerator performs modular exponentiations to support RSA and point multiplies to support ECC. At lower levels, the PKEU can perform simple operations such as modular multiplies.

1.3.2 Data Encryption Standard Execution Unit (DEU)

The DEU is used for bulk data encryption. It can also execute the Triple-DES algorithm, which is based on DES. The host processor supplies data to the DEU as input, and this data is encrypted and made available for reading. The session key is input to the DEU prior to encryption. The DEU computes the data encryption standard algorithm (ANSI X3.92) for bulk data encryption and decryption.

DES is a block cipher that uses a 56-bit key to encrypt 64-bit blocks of data, one block at a time. DES is a symmetric algorithm; therefore, each of the two communicating parties share the same 56-bit key. DES processing begins after this shared session key is agreed upon. The message to be encrypted (typically plain text) is partitioned into *n* sets of 64-bit blocks. Each block is processed, in turn, by the DES engine, producing *n* sets of encrypted (ciphertext) blocks. Decryption is handled in the reverse manner. The ciphertext blocks are processed one at a time by a DES module in the recipient's system. The same key is used, and the DEU manages the key processing internally so that the plaintext blocks are recovered.

The DES/3DES execution unit supports the following modes:

- ECB (electronic code book)
- CBC (cipher block chaining)

In addition to these modes, the DEU can compute Triple-DES. Triple-DES is an extension to the DES algorithm in which every 64-bit input block is processed three times. There are several ways that Triple-DES can be computed. The DES accelerator on the MPC180 supports two key (K1, K2, K1) or three key (K1, K2, K3) Triple-DES.

THe MPC180 supports two of the modes of operation defined for Triple-DES (see draft ANSI Standard X9.52-1998):

- TECB (Triple DES analogue of ECB)

- TCBC (Triple DES analogue of CBC)

1.3.3 Arc Four Execution Unit (AFEU)

The AFEU processes an algorithm that is compatible with the RC4 stream cipher from RSA Security, Inc. The RC4 algorithm is byte-oriented; therefore, a byte of plaintext is encrypted with a key to produce a byte of ciphertext. The key is variable length, and the AFEU supports 40-bit to 128-bit key lengths, providing a wide range of security levels. RC4 is a symmetric algorithm, so each of the two communicating parties share the same key.

AFEU processing begins after this shared session key is agreed upon. The plaintext message to be encrypted is logically partitioned into *n* sets of 8-bit blocks. In practice, the host processor groups 4 bytes at a time into 32-bit blocks and write that data to the AFEU. The AFEU internally processes each word one byte at a time. The AFEU engine processes each block in turn, byte by byte, producing *n* sets of encrypted (ciphertext) blocks. Decryption is handled in the reverse manner. The ciphertext blocks are processed one at a time by an AFEU in the recipient's system. The same key is used, and the AFEU manages the key processing internally so that the plaintext blocks are recovered.

The AFEU accepts data in 32-bit words per write cycle and produces 4 bytes of ciphertext for every 4 bytes of plaintext. Before any processing occurs, the key data is written to the AFEU, after which an initial permutation on the key happens internally. After the initial permutation is finished, processing on 32-bit words can begin.

1.3.4 Message Authentication Unit (MAU)

The MAU can perform SHA-1, MD5 and MD4, three of the most popular public message digest algorithms. At its simplest, the MAU receives 16 32-bit registers containing a message, and produces a hashed message of 128 bits for MD4/MD5 and 160 bits for SHA-1. The MAU also includes circuitry to automate the process of generating an HMAC (hashed message authentication code) as specified by RFC 2104. The HMAC can be built upon any of the hash functions supported by MAU.

1.3.5 Random Number Generator (RNG)

Because many cryptographic algorithms use random numbers as a source for generating a secret value, it is desirable to have a private RNG for use by the MPC180. The anonymity of each random number must be maintained, as well as the unpredictability of the next random number. The private RNG allows the system to develop random challenges or random secret keys. The secret key can thus remain hidden from even the high-level application code, providing an added measure of physical security. The RNG is also useful for digital signature generation.

The RNG is a digital integrated circuit capable of generating 32-bit random numbers. It is designed to comply with FIPS-140 standards for randomness and non-determinism. The RNG creates an unpredictable sequence of bits and assembles a string of those bits into a register. The random number in that register is accessible to the host through the host

interface of the RNG.

1.3.6 Software and Hardware Support

Customers will have access to device drivers integrated with the WindRiver VxWorks OS. Sample drivers will also be provided to customers wishing to integrate MPC180 support into other operating systems.

Third-party support for the MPC180 includes a development system for both the MPC860 and the MPC8260. The WindRiver/EST SBC8260C development system and Zephyr Engineering ZPC860C, both of which include a board support package, are available to accelerate customer design cycles.

Chapter 2
Signal Descriptions

This chapter provides a pinout diagram and signal descriptions for the MPC180 security processor.

2.1 Signal Descriptions

Table 2-1 groups pins by functionality.

Table 2-1. Pin Descriptions

Signal name	Pin locations	Signal type	Description
Signal pins			
A[18:29]	62, 64, 66, 67, 68, 70, 72–75, 77, 78	I	Address—address bus from the processor core. These bits are decoded in the MPC180 to produce the individual module select lines to the execution units. Note that the processor address bus might be 32 bits wide, while the MPC180 address bus is only 12 bits wide. msb = bit 0 lsb = bit 31
D[0:31]	1, 2, 4, 6, 7, 9, 11, 12, 14, 16-18, 20, 22, 24, 28–32, 34, 36, 37, 38, 87, 89, 90, 92, 94, 96, 98, 99	I/O	Data—bidirectional data bus. This bus is connected directly to the processor core. msb = bit 0 lsb = bit 31
$\overline{CS}$	56	I	Chip Select. Active low signal that indicates when a data transfer is intended for the MPC180.
R/$\overline{W}$	54	I	Read/Write. Read/write line 1 read cycle 0 write cycle
$\overline{BURST}$	55	I	Burst Transaction. Active low signal used in the 8260 interface that indicates when the current read/write is a burst transfer.
$\overline{TS}$	53	I	Transfer Start. Transfer start pin for control port. This signal is asserted by the 850/860 to indicate the start of a bus cycle that transfers data to or from the MPC180. This is used by the MPC180 along with $\overline{CS}$, R/$\overline{W}$, and A to begin a transfer.

Table 2-1. Pin Descriptions (Continued)

Signal name	Pin locations	Signal type	Description
PSDVAL	82	I	Data valid. This active low signal is ignored when CONFIG=0 (MPC860 Mode), but is active in MPC8260 Mode. The assertion of PSDVAL indicates that a data beat is valid on the data bus.
TA / LUPMWAIT	61	O	Transfer Acknowledge. This active low signal is used in 860 mode and is asserted by the MPC180 when a successful read or write has occurred. Local UPM wait. This active high signal is used in 8260 mode and is asserted to indicate the number of wait states for a transaction.
Miscellaneous pins			
RESET	52	I	Reset. Asynchronous reset signal for initializing the chip to a known state. It is highly recommended that this signal be connected to a dual hardware/software reset function. Thus, the system designer can reset the MPC180 chip with optimal flexibility.
CONFIG	57	I	Configuration. Input that indicates whether the interface is to an MPC860 or MPC8260 1 8260 interface 0 860 interface
ENDIAN	40	I	Endian. Active high for big endian mode. Low for little endian mode. 1 big endian 0 little endian
IRQ	85	O	Interrupt Request. Interrupt line that signifies that one or more execution units modules has asserted its IRQ hardware interrupt.
NC	26, 27, 49, 50, 51, 76, 100	—	No connection to the pin
DMA Hardware Handshake pins			
DREQ1	83	O	DMA Request 1. Active high signal which indicates that either the input or output buffer is requesting data transfer by the host or DMA controller. DREQ1 and DREQ2 are each programmable to refer to the MPC180 chip input buffer or output buffer. This signal is designed to interoperate with a PowerQUICC IDMA channel.
DREQ2	84	O	DMA request 2. Active high signal which indicates that either the input or output buffer is requesting data transfer by the host or DMA controller. DREQ1 and DREQ2 are each programmable to refer to the MPC180 Chip input buffer or output buffer. This signal is designed to interoperate with a PowerQUICC IDMA channel.
Clock			
CLK	59	I	Master clock input
Test			
TCK	47	I	JTAG test clock
TDI	48	I	JTAG test data input
TDO	44	I	JTAG test data output
TMS	46	I	JTAG test mode select
TRST	45	I	JTAG test reset

Table 2-1. Pin Descriptions (Continued)

Signal name	Pin locations	Signal type	Description
Power and Ground			
IVDD	10, 21, 41, 60, 71, 93	I	+1.8 Volts (power pins for core logic)
OVDD	5, 15, 25, 35, 43, 65, 81, 88, 97	I	+3.3 Volts (Power pins for I/O pads)
OVSS	3, 13, 23, 33, 42, 63, 79, 80, 86, 95	I	0 Volts (Ground)
IVSS	8, 19, 39, 58, 69, 91	I	0 Volts (Ground)

Figure 2-1 shows the MPC180 pinout.

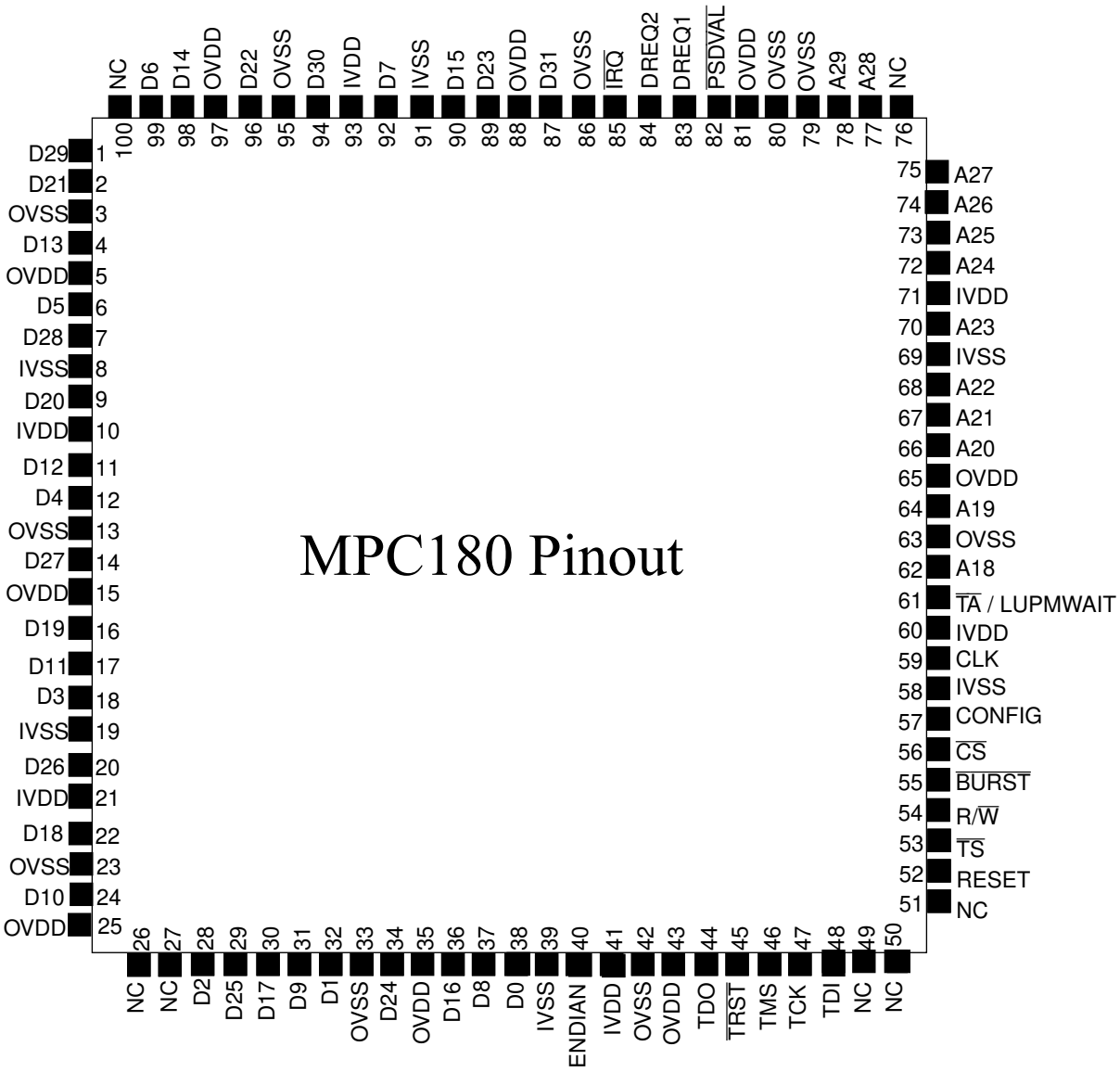

Figure 2-1. MPC180 Pin Diagram

Chapter 3
External Bus Interface and Memory Map

This chapter describes the MPC180 address map, the External Bus Interface (EBI), and EBI registers.

3.1 Execution Unit Registers

Each MPC180 execution unit has a dedicated set of registers. The MPC180 has a unified memory map that allows software addressibility to all internal registers. Figure 3-1 lists each MPC180 register and its 12-bit MPC180 chip address.

PKEU

A00	BRAM [64x32]
A40	ARAM [64x32]
A80	NRAM[64x32]
B00	EXP(k)
B01	Control [CR]
B02	Status [SR]
B03	Mask [MR]
B04	Instruction [IR]
B05	Prog. counter [PC]
B06	Clear interrupt
B07	Modulus size
B08	EXP(k) size
B09	Device ID

MDEU

000	MDMB [0–15]
010	Digest [0–4]
015	Control [CR]
016	Status [SR]
017	Clear interrupt
018	Device ID

DEU

200	Control
201	Status
202	Key1-right
203	Key1-left
204	Key2-right
205	Key2-left
206	Key3-right
207	Key3-left
208	IV-right
209	IV-left
20A	DATAIN_R
20B	DATAIN_L
20C	DATAOUT_R
20D	DATAOUT_L
20E	Configuration

RNG

600	Command/status
602	AutoRand output

EBI

A00	Input buffer
A80	Output buffer
B00	CSTAT
B01	ID register
B02	IMASK
B03	IBCTL
B04	IBCNT
B05	OBCTL
B06	OBCNT

AFEU

400	Control
401	Status
402	Clear interrupt
403	Key length
404	Key data[0–3]
408	Last sub msg
409	Plaintext-in
40A	Ciphertext-out
40B	Context I/J
410	Context SBox[0–63]

Figure 3-1. MPC180 Execution Unit Registers

Most of these registers are read and write, however some have special permissions. See Table 3-1 for more information. The 12-bit MPC180 address of each register is shown next to the register name. All registers are assumed to be 32 bits wide; however, registers that contain fewer bits will return 0 (or a known value) on unused bits for that bus transaction only. Many registers contain multiple 32-bit words. If so, the number of words in the register set is shown in brackets after the name. Individual execution unit chapters describe how to use these registers, the bit assignments, and bit ordering.

3.2 Address Map

Table 3-1 lists the addresses for all registers in each execution unit. The 12-bit MPC180 address bus value is shown along with a 32-bit host processor address bus value.

Table 3-1. 32-Bit System Address Map

MPC180 12-Bit Address	Processor 32-Bit Address	Register	Type
MDEU: 0x000–0x1FF			
0x000	0x0000_0000	Message buffer(MB0)	W
0x001	0x0000_0004	Message buffer(MB1)	W
0x002	0x0000_0008	Message buffer(MB2)	W
0x003	0x0000_000C	Message buffer(MB3)	W
0x004	0x0000_0010	Message buffer(MB4)	W
0x005	0x0000_0014	Message buffer(MB5)	W
0x006	0x0000_0018	Message buffer(MB6)	W
0x007	0x0000_001C	Message buffer(MB7)	W
0x008	0x0000_0020	Message buffer(MB8)	W
0x009	0x0000_0024	Message buffer(MB9)	W
0x00A	0x0000_0028	Message buffer(MB10)	W
0x00B	0x0000_002C	Message buffer(MB11)	W
0x00C	0x0000_0030	Message buffer(MB12)	W
0x00D	0x0000_0034	Message buffer(MB13)	W
0x00E	0x0000_0038	Message buffer(MB14)	W
0x00F	0x0000_003C	Message buffer(MB15)	W
0x010	0x0000_0040	Message digest (MA)	R/W
0x011	0x0000_0044	Message digest (MB)	R/W
0x012	0x0000_0048	Message digest (MC)	R/W
0x013	0x0000_004C	Message digest (MD)	R/W
0x014	0x0000_0050	Message digest (ME)	R/W
0x015	0x0000_0054	Control (MCR)	R/W
0x016	0x0000_0058	Status (MSR)	R/W
0x017	0x0000_005C	Clear interrupt (MCLRIRQ)	W

Table 3-1. 32-Bit System Address Map (Continued)

MPC180 12-Bit Address	Processor 32-Bit Address	Register	Type
0x018	0x0000_0060	Version Identification (MID)	R
DEU: 0x200–0x3FF			
0x200	0x0000_0800	Control (DCR)	R/W
0x201	0x0000_0804	Status (DSR)	R
0x202	0x0000_0808	Key1_R	R/W
0x203	0x0000_080C	Key1_L	R/W
0x204	0x0000_0810	Key2_R	R/W
0x205	0x0000_0814	Key2_L	R/W
0x206	0x0000_0818	Key3_R	R/W
0x207	0x0000_081C	Key3_L	R/W
0x208	0x0000_0820	IV_R	R/W
0x209	0x0000_0824	IV_L	R/W
0x20A	0x0000_0828	DATAIN_R	R/W
0x20B	0x0000_082C	DATAIN_L	R/W
0x20C	0x0000_0830	DATAOUT_R	R
0x20D	0x0000_0834	DATAOUT_L	R
0X20E	0x0000_0838	Configuration (DCFG)	R/W
AFEU: 0x400–0x5FF			
0x400	0x0000_1000	Control	W
0x401	0x0000_1004	Status	R
0x402	0x0000_1008	Clear interrupt	W
0x403	0x0000_100C	Key Length	W
0x404	0x0000_1010	Key Low	W
0x405	0x0000_1014	Key Lower-Middle	W
0x406	0x0000_1018	Key Upper-Middle	W
0x407	0x0000_101C	Key Upper	W
0x408	0x0000_1020	Message Byte Double Word	W
0x409	0x0000_1024	Plaintext-in	W
0x40A	0x0000_1028	Ciphertext-out	R
0x40B	0x0000_102C	S-box I/J	R/W
0x410	0x0000_1040	SBox [0]	R/W
0x414	0x0000_1050	SBox [1]	R/W
0x418	0x0000_1060	SBox [2]	R/W
...	...	...	...
0x50C	0x0000_1430	SBox [63]	R/W