

Preliminary Information

MPC184PCIHWRM/D  
Rev. 2.1, 4/2003

MPC184 PCI Mode Hardware  
Reference Manual



*Matthew Short*  
*Security Applications*  
matt.short@motorola.com

This document describes how to design a system with the MPC184 in a 32bit PCI environment. It also describes how to design a system to quickly transition from the MPC190 in 32b mode to the MPC184. It covers the following topics:

<b>Topic</b>	<b>Page</b>
Section 1, "Overview"	2
Section 2, "System Architecture"	3
Section 3, "Pin Assignments"	4
Section 4, "Signal Descriptions"	4
Section 5, "Electrical and Thermal Characteristics"	7
Section 6, "Case Outline Package Dimensions"	12

# 1 Overview

The MPC184 is a flexible and powerful addition to any networking or computing system using the Motorola PowerQUICC line of integrated communications processors, or any system supporting the PCI bus protocol. The MPC184 is designed to off load computationally intensive security functions, such as key generation and exchange, authentication, and bulk encryption from the host processor.

The MPC184 is optimized to process all the algorithms associated with IPsec, IKE, WTLS/WAP and SSL/TLS. In addition, the Motorola family of security co-processors are the only devices on the market capable of executing elliptic curve cryptography which is especially important for secure wireless communications.

MPC184 features include the following:

- 1 Public key execution units (PKEUs) that support the following:
  - RSA and Diffie-Hellman
    - Programmable field size up to 2048-bits
  - Elliptic curve cryptography
    - $F_{2^m}$  and  $F(p)$  modes
    - Programmable field size up to 511-bits
- 1 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
- 1 Advanced Encryption Standard unit (AESU)
  - Implements the Rijndael symmetric key cipher
  - Implements ECB, CBC and Counter modes
- 1 ARC Four execution unit (AFEU)
  - Implements a stream cipher compatible with the RC4 algorithm
  - 40- to 128-bit programmable key
- 1 Message digest execution units (MDEUs)
  - SHA-1 with 160-bit or 256-bit message digest
  - MD5 with 128-bit message digest
  - HMAC with either algorithm
- 1 Random number generator (RNG)
- 8xx compliant external bus interface, with master/slave logic.
  - 32-bit address/32-bit data
  - 75 MHz operation
- PCI 2.2 compliant external bus interface, with master/slave logic
  - 32-bit address/32-bit data mode, 66MHz
- 4 Crypto-channels, each supporting multi-command descriptor chains
  - Static and/or dynamic assignment of crypto-execution units via an integrated controller
- 8KB of internal scratchpad memory for key, IV and context storage
- 1.5V supply, 3.3V I/O
- 252 MAP BGA
- 1.0W power dissipation

## 2 System Architecture

The MPC184 is designed to integrate easily into any system using the 8xx or PCI bus protocol. The MPC184 is ideal in any system using a Motorola PowerQUICC communications processor (as shown in Figure 1) or any system with 32b PCI such as the Motorola MPC8245 integrated processor (see Figure 2). The ability of the MPC184 to be a master on the 8xx or PCI bus allows the co-processor to offload the data movement bottleneck normally associated with slave devices. The external processor accesses the MPC184 through its device drivers using system memory for data storage. The MPC184 resides in the memory map of the processor, therefore when an application requires cryptographic functions, it simply creates descriptors for the MPC184 which define the cryptographic function to be performed and the location of the data. The MPC184's mastering capability permits the host processor to set up a crypto-channel with a few short register writes, leaving the MPC184 to perform reads and writes on system memory to complete the required task.

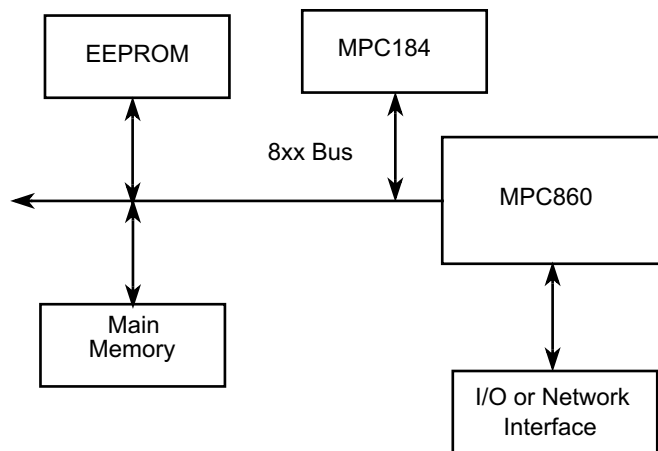


Figure 1. MPC184 Connected to PowerQuicc 8xx Bus

Figure 2 shows the MPC184 communicating with an integrated processor such as the MPC8245.

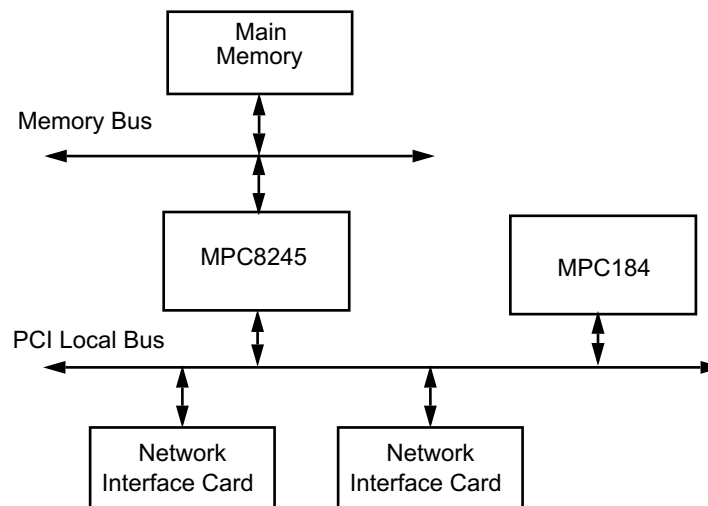


Figure 2. MPC184 Connected to an integrated Host CPU such as the MPC8245

### 3 Pin Assignments

Table 1 shows the pin connections for the MPC184 in 32 bit PCI mode. The shaded regions show the pins that MUST be No Connected in 32b PCI mode or must be taken into special consideration for easy migration from the MPC190.

Table 1. MPC184 Pin Diagram

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
<b>A</b>		TMS	TCK	TRST	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC		<b>A</b>
<b>B</b>	TDO	VSS	VSS	VSS	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	<b>B</b>
<b>C</b>	TDI	VSS	VSS	VSS	VSS	3.3V	VSS	3.3V	3.3V	VSS	3.3V	VSS	VSS	VSS	NC	NC	<b>C</b>
<b>D</b>	INTA	GNT	VSS	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	NC	NC	<b>D</b>
<b>E</b>	RST#	M66EN	3.3V	3.3V	Core V	Core V	Core V	Core V	Core V	Core V	Core V	Core V	3.3V	VSS	NC	NC	<b>E</b>
<b>F</b>	REQ#	Analog Vdd	3.3V	3.3V	Core V	VSS	VSS	VSS	VSS	VSS	VSS	Core V	3.3V	VSS	NC	NC	<b>F</b>
<b>G</b>	VSS	TPA /NC	VSS	3.3V	Core V	VSS	VSS	VSS	VSS	VSS	VSS	Core V	3.3V	3.3V	NC	NC	<b>G</b>
<b>H</b>	CLK	AVSS	3.3V	3.3V	Core V	VSS	VSS	VSS	VSS	VSS	VSS	Core V	3.3V	3.3V	NC	NC	<b>H</b>
<b>J</b>	VSS	VSS	3.3V	3.3V	Core V	VSS	VSS	VSS	VSS	VSS	VSS	Core V	3.3V	VSS	NC	NC	<b>J</b>
<b>K</b>	AD_30	AD_31	3.3V	3.3V	Core V	VSS	VSS	VSS	VSS	VSS	VSS	Core V	3.3V	3.3V	NC	NC	<b>K</b>
<b>L</b>	AD_28	AD_29	VSS	3.3V	Core V	VSS	VSS	VSS	VSS	VSS	VSS	Core V	3.3V	3.3V	AD_1	AD_0	<b>L</b>
<b>M</b>	AD_26	AD_27	3.3V	3.3V	Core V	Core V	Core V	Core V	Core V	Core V	Core V	Core V	3.3V	VSS	AD_3	AD_2	<b>M</b>
<b>N</b>	AD_24	AD_25	VSS	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	3.3V	AD_5	AD_4	<b>N</b>
<b>P</b>	IDSEL	C/BE_3	VSS	VSS	PLL Bypass	VSS	VSS	3.3V	VSS	3.3V	VSS	VSS	VSS	VSS	AD_7	AD_6	<b>P</b>
<b>R</b>	AD_23	AD_22	VSS	VSS	AD_18	AD_16	FRAME	TRDY	STOP	PERR	PAR	AD_15	AD_13	AD_11	AD_8	C/BE_0	<b>R</b>
<b>T</b>		AD_21	AD_20	AD_19	AD_17	C/BE_2	IRDY	DEVSEL	3.3V	SERR	C/BE_1	AD_14	AD_12	AD_10	AD_9		<b>T</b>
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	

### 4 Signal Descriptions

Table 2 shows the signal descriptions for the MPC184 in 32 bit PCI mode. The shaded regions show the pins that MUST be No Connected in 32b PCI mode or must be taken into special consideration for easy migration from the MPC190. Please also reference Chapter 2, 4 and 7 of the PCI Local Bus Specification Revision 2.2 for other PCI system considerations.

**Table 2. Signal Descriptions**

Signal Name	Pin Locations	Signal Type	Type	Description
<b>Address/Data and Command Pins (37)</b>				
AD[31:0]	K2, K1, L2, L1, M2, M1, N2, N1, R1, R2, T2, T3, T4, R5, T5, R6, R12, T12, R13, T13, R14, T14, T15, R15, P15, P16, N15, N16, M15, M16, L15, L16	I/O	T/S	Multiplexed Address/Data Bus
C/BE[3-0]#	P2, T6, T11, R16	I/O	T/S	Bus Command/Byte Enables
PAR	R11	I/O	T/S	Parity (Even Parity across AD[31:0], C/BE [3:0])
<b>Interface Control (7)</b>				
FRAME#	R7	I/O	S/T/S	Assertion of FRAME# by an Initiator indicates the beginning of a bus transaction. FRAME is deasserted 1 cycle before conclusion of the transaction.
TRDY#	R8	I/O	S/T/S	Assertion of TRDY# by a target indicates readiness to complete a bus transaction.
IRDY#	T7	I/O	S/T/S	Assertion of IRDY# by an Initiator indicates readiness to complete a bus transaction.
STOP#	R9	I/O	S/T/S	Asserted by a target to request termination a bus transaction.
IDSEL	P1	I	IN	Initialization device select is used as chip select pin during Type 0 configuration transactions.
DEVSEL#	T8	I/O	S/T/S	Asserted by a target when claiming a transaction (following subtractive decode of its address).
M66EN	E2	I	IN	When asserted (at initialization time), the MPC184 enables its internal PLL to operate in the 33-66MHz range.
PLL Bypass	P5	I	IN	PLL Bypass 0 (OVSS) = PLL Disabled 1 (OVDD) = PLL Enabled
<b>Arbitration (2)</b>				
REQ#	F1	O	T/S	Bus Request from Initiator to Arbiter
GNT#	D2	I	T/S	Bus Grant from Arbiter to Initiator
<b>System (3)</b>				
CLK	H1	I	IN	System Clock input
RST#	E1	I	IN	Asynchronous reset signal. Initializes MPC184 to known state.
TPA	G2	O		Test Pad Analog This pin MUST have No Connection
<b>Error Reporting (2)</b>				

**Table 2. Signal Descriptions (continued)**

Signal Name	Pin Locations	Signal Type	Type	Description
SERR#	T10	O	O/D	System Error is active low when unrecoverable system error is detected.
PERR#	R10	I/O	S/T/S	Parity Error is active low when Parity Error is detected
<b>Interrupt Signals (1)</b>				
INTA#	D1	O	O/D	Interrupt Request
<b>JTAG/Boundary Scan (5)</b>				
TCK	A3	I		Test Clock If JTAG is NOT used, this pin must be tied to VSS
TDI	C1	I		Test Input If JTAG is NOT used, this pin must be tied to OVDD
TDO	B1	O		Test output If JTAG is NOT used, this pin must be NC
TMS	A2	I		Test Mode Select If JTAG is NOT used, this pin must be tied to OVDD
TRST#	A4	I		Test Reset If JTAG is NOT used, this pin must be tied to VSS
<b>Powers/Grounds/No Connects (195)</b>				
Analog VDD	F2			Analog PLL Power MPC184 = +1.5 V MPC190 = +1.8 V
AVSS	H2			Analog PLL Ground
VSS	B2, B3, B4, C2, C3, C4, C5, C7, C10, C12, C13, C14, D3, E14, F6, F7, F8, F9, F10, F11, F14, G1, G3, G6, G7, G8, G9, G10, G11, H6, H7, H8, H9, H10, H11, J1, J2, J6, J7, J8, J9, J10, J11, J14, K6, K7, K8, K9, K10, K11, L3, L6, L7, L8, L9, L10, L11, M14, N3, P3, P4, P6, P7, P9, P11, P12, P13, P14, R3, R4			Ground
IVDD	E5, E6, E7, E8, E9, E10, E11, E12, F5, F12, G5, G12, H5, H12, J5, J12, K5, K12, L5, L12, M5, M6, M7, M8, M9, M10, M11, M12			Core Power MPC184 = +1.5 V MPC190 = +1.8 V

**Table 2. Signal Descriptions (continued)**

Signal Name	Pin Locations	Signal Type	Type	Description
OVDD	C6, C8, C9, C11, D4, D5, D6, D7, D8, D9, D10, D11, D12, D13, D14, E3, E4, E13, F3, F4, F13, G4, G13, G14, H3, H4, H13, H14, J3, J4, J13, K3, K4, K13, K14, L4, L13, L14, M3, M4, M13, N4, N5, N6, N7, N8, N9, N10, N11, N12, N13, N14, P8, P10, T9			I/O Power (+3.3v)
NC	G16, F15, F16, E15, E16, D15, D16, C15, C16, B15, B16, A15, B14, A14, B13, A13, B12, A12, B11, A11, B10, A10, B9, A9, B8, A8, B7, A7, B6, A6, B5, A5, J15, J16, H15, H16, G15, K16, K15			These pins MUST have No Connection

## 5 Electrical and Thermal Characteristics

This chapter provides the AC and DC electrical specifications as well as the thermal characteristics of the MPC184.

### 5.0.1 Absolute Maximum Ratings

Table 3 lists ranges of absolute maximums of the MPC184.

**Table 3. Absolute Maximum Ratings**

Characteristic	Name	Absolute Min	Absolute Max	Unit
Power supply voltage—Core	V <sub>DD</sub>	-0.5	+2.0	Volts
Power supply voltage—I/O	V <sub>DDQ</sub>	-0.5	+4.1	Volts
Storage temperature	—	-55	+125	°C
Static input pin voltage	—	-0.4	+4.1	Volts

**Note:** V<sub>DDQ</sub> must not exceed V<sub>DD</sub> by more than 2.2V at any time.

**Note:** Permanent device damage may occur if ABSOLUTE MAXIMUM RATINGS are exceeded. Functional operation should be restricted to RECOMMENDED OPERATING CONDITIONS. Exposure to higher than recommended voltages for extended periods of time could affect device reliability.

**Note:** This device contains circuitry to protect the inputs against damage due to high static voltages or electric fields; however, it is advised that normal precautions be taken to avoid application of any voltage higher than maximum rated voltages to this high-impedance circuit.

### 5.0.2 Package Thermal Characteristics

Table 4 shows thermal resistances for the 252-pin MBGA package.

**Table 4. Package Thermal Characteristics**

Rating		Symbol	Max	Unit
Junction to ambient <sup>1,2</sup> (@1m/s)	Single-layer board	R	24	°C/W
	Four-layer board		18	
Junction to board <sup>3</sup> (bottom)		R	12	°C/W
Junction to case <sup>4</sup> (top)		R	6	°C/W

<sup>1</sup> Junction temperature is a function of on-chip power dissipation, package thermal resistance, mounting site (board) temperature, ambient temperature, air flow, board population, and board thermal resistance.

<sup>2</sup> Per SEMI G38-87.

<sup>3</sup> Indicates the average thermal resistance between the die and the printed circuit board via the cold-plate method, per JESD 51-8.

<sup>4</sup> Indicates the average thermal resistance between the die and the case top surface via the cold plate method (MIL SPEC-883 Method 1012.1).

### 5.0.3 Operating Conditions and Electrical Characteristics

Table 5 shows AC and DC electrical characteristics. Unless specified otherwise, conditions are as follows:

$V_{SS} = 0$  V DC and  $T_A = 0^\circ$  C to  $120^\circ$  C.

**Table 5. DC Electrical Characteristics**

Characteristic	Name	Min	Max	Units
Power supply voltage—Core	$V_{DD}$	1.35	1.65	$V_{DC}$
Power supply voltage—I/O	$V_{DDQ}$	3.0	3.6	$V_{DC}$
Input low voltage ( $V_{dd} = \text{min}$ )	$V_{il}$	-0.5	$0.3 V_{DDQ}$	$V_{DC}$
Input high voltage ( $V_{dd} = \text{max}$ )	$V_{ih}$	$0.5 V_{DDQ}$	$V_{DDQ} + 0.5$	$V_{DC}$
AC supply current (I/O power not included)	$I_{DD}$	—	400	mA
Standby supply current	$I_{SS}$	—	150	mA
Input leakage current @ $V_{DDQ} \geq V_{in} \geq V_{SS}$	$I_{leak}$	—	$\pm 10$	$\mu A$
Output high voltage ( $I_{oh} = -500 \mu A$ )	$V_{oh}$	$0.9 V_{DDQ}$	—	$V_{DC}$
Output low voltage ( $I_{OL} = 1500 \mu A$ ) $I_{ol} = 3.2$ mA, $C_L = 35$ pF (IRQ) $I_{ol} = 3.2$ mA, $C_L = 50$ pF (D[0:31])	$V_{ol}$	—	$0.1 V_{DDQ}$	$V_{DC}$
Output high current <sup>1</sup>	$I_{OH}(AC)$	$-12 V_{DDQ}$	$-32 V_{DDQ}$	$\mu A$
Output low current <sup>2</sup>	$I_{OL}(AC)$	$16 V_{DDQ}$	$38 V_{DDQ}$	$\mu A$

<sup>1</sup>  $V_{OUT} = 0.3 V_{DDR}$  for  $I_{OH}$  (min),  $V_{OUT} = 0.7 V_{DDQ}$  for  $I_{OH}$  (max)

<sup>2</sup>  $V_{OUT} = 0.6 V_{DDR}$  for  $I_{OL}$  (min),  $V_{OUT} = 0.18 V_{DDQ}$  for  $I_{OL}$  (max)

### 5.0.4 AC Timing Specifications

Table 6 shows the AC timing specifications for the master clock and reset signals. Unless specified otherwise, conditions are as follows:



1.65 V ≤ IVDD ≤ 1.95 V; VSS = 0 V; T A = 0° C to 70° C, ± 5%.

**Table 6. AC Timing Specifications—Clock and Reset Pins**

Condition	Name	Min	Typ	Max	Units
Output rise/fall time	T <sub>rfc</sub>	—	—	3	nS
MCLK frequency	F <sub>C</sub>	—	66	—	MHz
MCLK duty cycle	F <sub>dc</sub>	45	50	55	%
RESET pulse width	T <sub>rst</sub>	16	—	—	cycles
RESET input rise/fall time	T <sub>rfr</sub>	—	—	1	μS

## 5.0.5 AC Timing Characteristics

Table 7 shows the AC timing specifications for data signals.

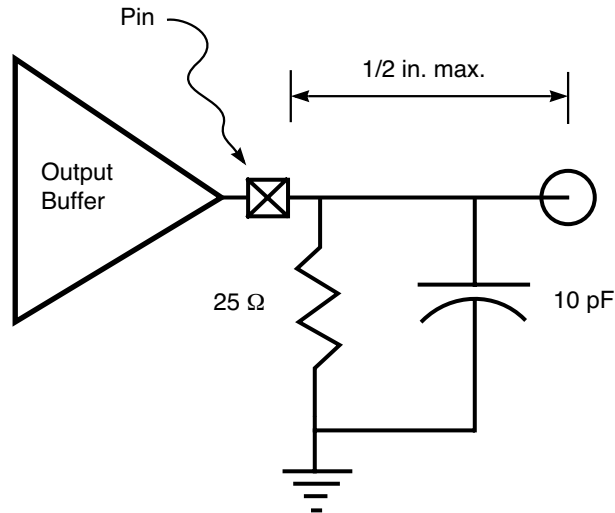
**Table 7. AC Electrical Characteristics**

Condition	Name	Min	Max	Units
<b>Input Signals</b>				
Clock frequency	F <sub>clock</sub>	—	66	Mhz
Clock cycle time	t <sub>cyc</sub>	15	—	nS
Clock-to-signal valid delay <sup>1, 2</sup>	t <sub>val</sub>	2	6	nS
Input setup time to clock-based signals	t <sub>su</sub>	3	—	nS
Input setup time to clock point-to-point signals	t <sub>su</sub> (Pip)	5	—	nS
Input hold time clock	t <sub>n</sub>	0	—	nS
Float to active delay	t <sub>on</sub>	2	—	nS
Active to float delay	t <sub>off</sub>	—	14	nS

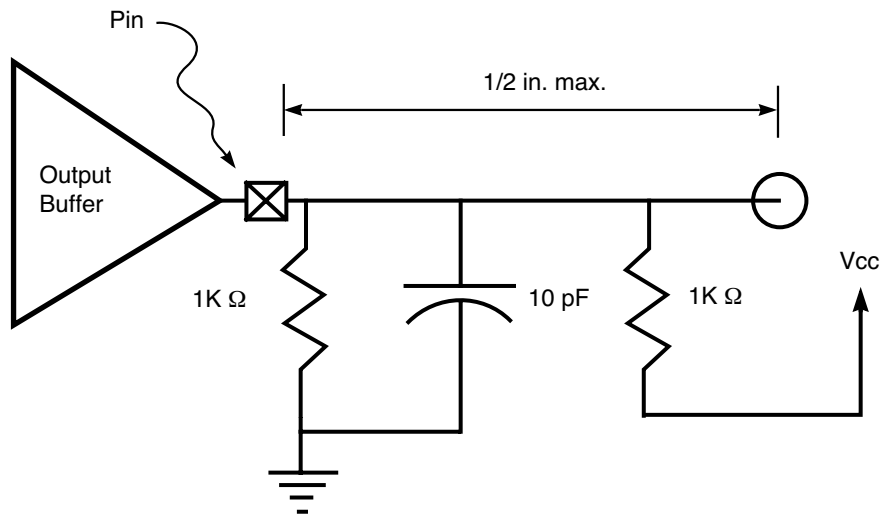
<sup>1</sup> Maximum times are measured with the circuit load shown in Figure 3 and Figure 5.

<sup>2</sup> Minimum times are measured at the package pin with the circuit load shown in Figure 4.

Figure 3, Figure 4, and Figure 5 show timing circuits.



**Figure 3.  $T_{val}$  (max) Rising Edge**



**Figure 4.  $T_{val}$  (min) and Slew Rate**

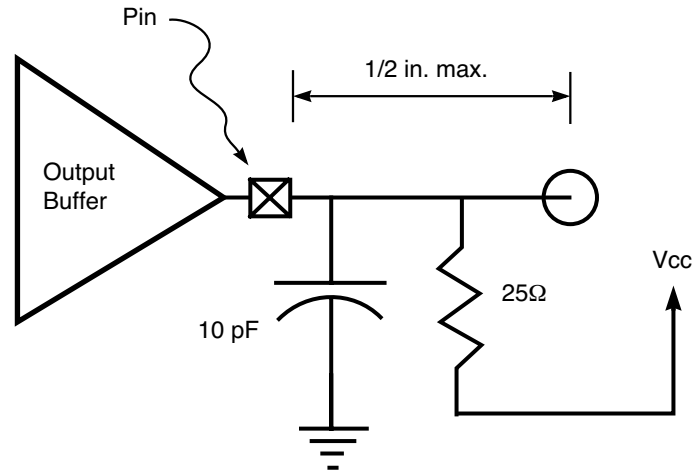


Figure 5.  $T_{val}$  (max) Falling Edge

## 5.0.6 IEEE 1149.1 AC Timing Specifications

All units in Table 8 are nanoseconds.

Table 8. JTAG AC Timing Specifications

Condition	Name	Min	Max
TCK cycle time	$t_{THTH}$	60	—
TCK clock high time	$t_{TH}$	25	—
TCK clock low time	$t_{TL}$	25	—
TDO access time	$t_{TLQV}$	1	10
$\overline{TRST}$ pulse width	$t_{TSRT}$	40	—
Setup times Capture	$t_{CS}$	5	—
	TDI $t_{DVTH}$	5	—
	TMS $t_{MVTH}$	5	—
Hold times Capture	$t_{CH}$	13	—
	TDI $t_{THDX}$	14	—
	TMS $t_{THMX}$	14	—

## 6 Case Outline Package Dimensions

Figure 6 and Figure 7 show the case outline package dimensions.

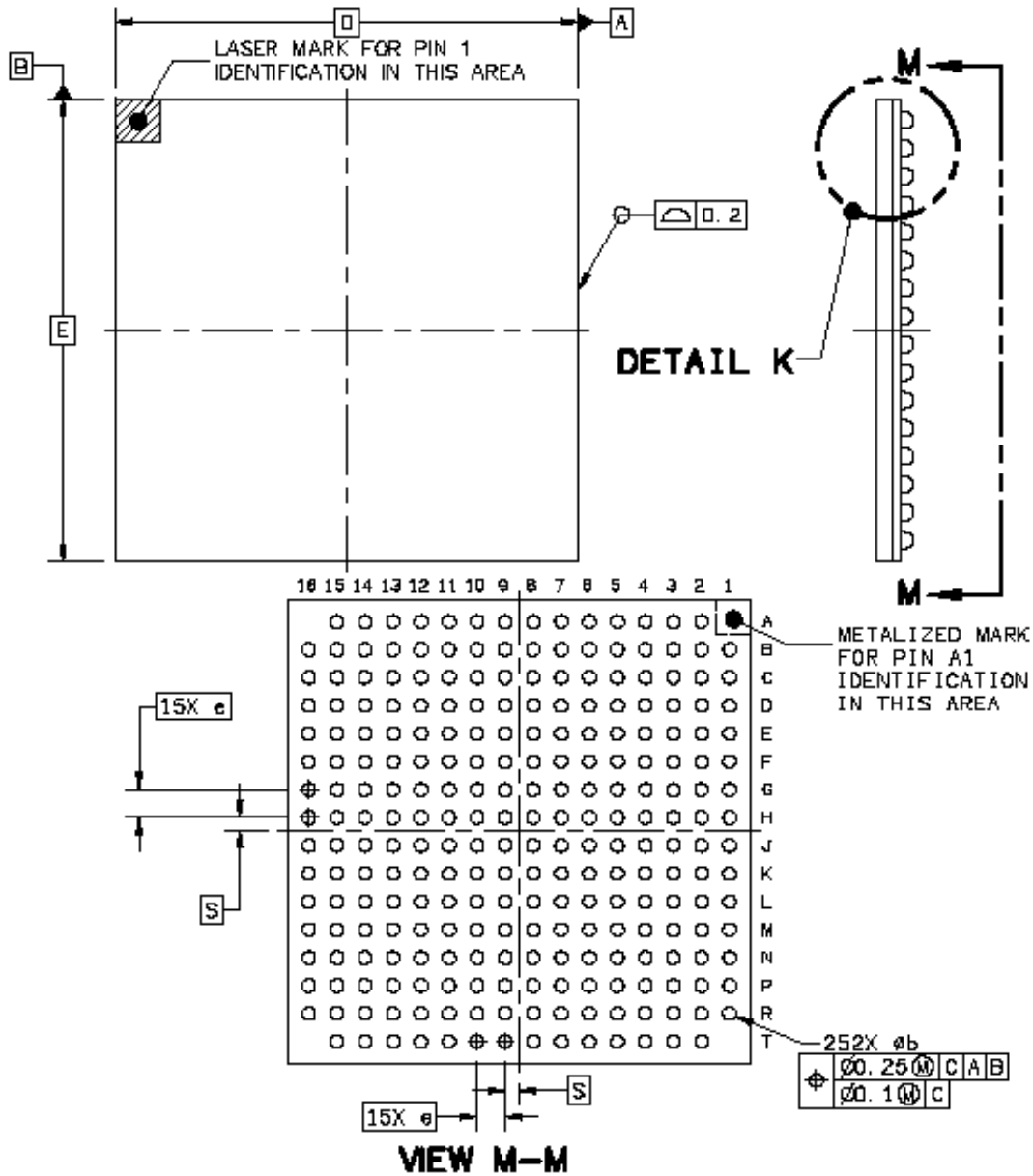


Figure 6. Case Dimensions

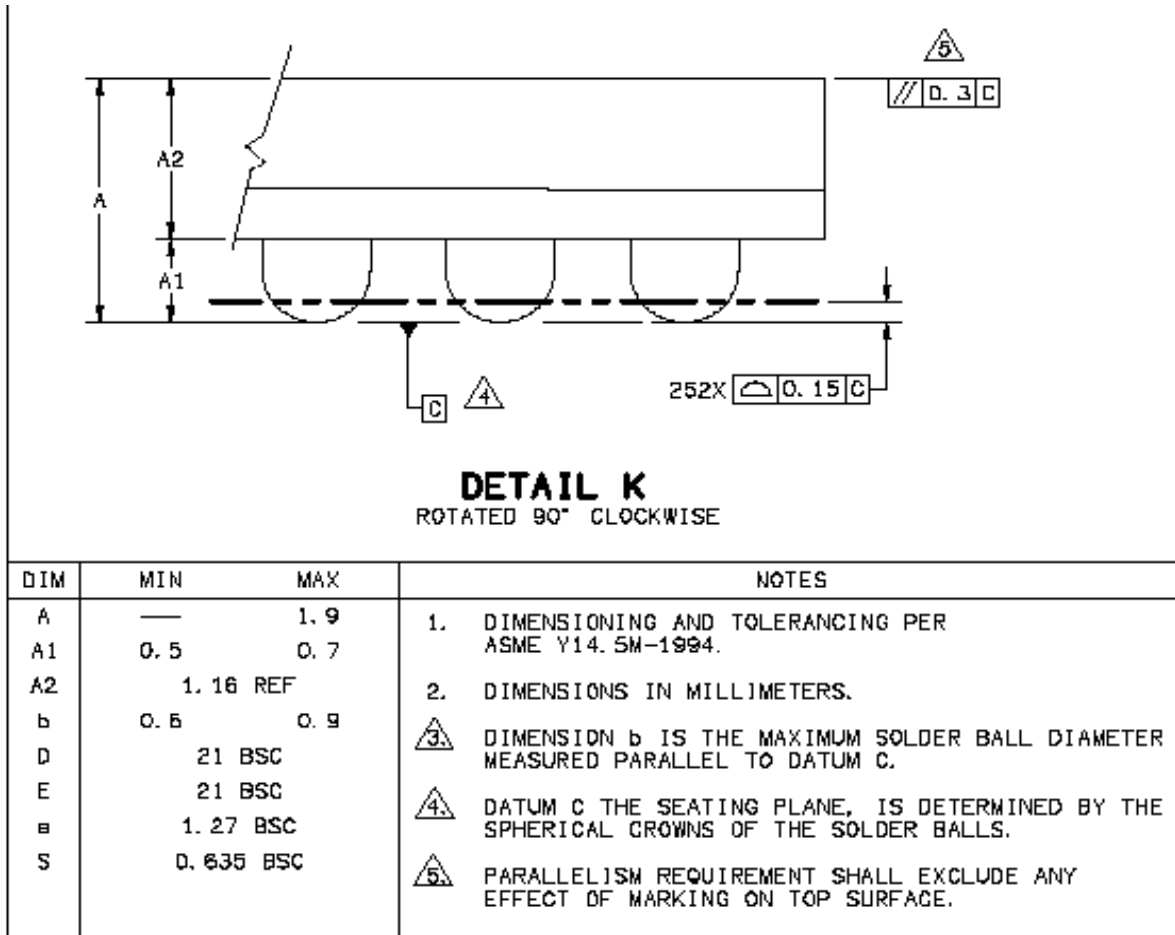


Figure 7. Detail of Case Dimensions

THIS PAGE INTENTIONALLY LEFT BLANK

THIS PAGE INTENTIONALLY LEFT BLANK

# Freescale Semiconductor, Inc.

## HOW TO REACH US:

### USA/EUROPE/LOCATIONS NOT LISTED:

Motorola Literature Distribution  
P.O. Box 5405, Denver, Colorado 80217  
1-480-768-2130  
(800) 521-6274

### JAPAN:

Motorola Japan Ltd.  
SPS, Technical Information Center  
3-20-1, Minami-Azabu Minato-ku  
Tokyo 106-8573 Japan  
81-3-3440-3569

### ASIA/PACIFIC:

Motorola Semiconductors H.K. Ltd.  
Silicon Harbour Centre, 2 Dai King Street  
Tai Po Industrial Estate, Tai Po, N.T., Hong Kong  
852-26668334

### TECHNICAL INFORMATION CENTER:

(800) 521-6274

### HOME PAGE:

[www.motorola.com/semiconductors](http://www.motorola.com/semiconductors)

Information in this document is provided solely to enable system and software implementers to use Motorola products. There are no express or implied copyright licenses granted hereunder to design or fabricate any 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 which may be provided in Motorola data sheets and/or specifications can and do vary in different applications and actual performance may vary over time. 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 the Stylized M Logo are registered in the U.S. Patent and Trademark Office. digital dna is a trademark of Motorola, Inc. The PowerPC name is a trademark of IBM Corp. and used under license. All other product or service names are the property of their respective owners. Motorola, Inc. is an Equal Opportunity/Affirmative Action Employer.

© Motorola, Inc. 2003

MPC184PCIHWRM/D

**For More Information On This Product,  
Go to: [www.freescale.com](http://www.freescale.com)**



[Freescale](#) > [Security Processors](#) > [S1 Family](#) > MPC184

MPC184 : Security Processor

[SUBSCRIBE](#)

The MPC184 security processor is optimized for any system supporting Freescale's 8xx bus and the 32-bit PCI interface standard. It is designed to off-load computational intensive security functions, such as key generation and exchange, authentication and bulk encryption from processors such as Freescale's MPC8xx and MPC824x family of integrated host processors, or from any processor through the use of a PCI bridge chip. Typical applications include SOHO/ROBO routers, DSLAMS, Broadband access equipment, e-commerce servers and WAP gateways.

**Rate this Page**

-- - 0 + ++

[Care to Comment?](#)

▶ [Block Diagram](#)

## MPC184 Features

- 1 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
- 1 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
- 1 Advanced Encryption Standard unit (AESU)
  - Programmable key length of 128, 192, or 256-bits
  - Implements the Rijndael symmetric key cipher
  - Support for ECB, CBC, and counter modes
- 1 ARC Four execution unit (AFEU)
  - Implements a stream cipher compatible with the RC4 algorithm
  - 40- to 128-bit programmable key
- 1 Message digest execution units (MDEUs)
  - 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
- 1 Random number generator (RNG)

- 8xx compliant external bus interface, with master/slave logic
  - 32-bit address/32-bit data
  - Up to 75 MHz operation
- PCI 2.2 compliant external bus interface, with master/slave logic
  - 32-bit address/32-bit data mode, 66 MHz
- 4 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 execution unit, with flow control for large data sizes
- 8 KB of internal scratchpad memory for key, IV and context storage
- 1.0W power dissipation
- Software and development support available

▲ [Return to Top](#)

Operating Frequency (Max) (MHz)	Core Operating Voltage (Spec) (V)	I/O Operating Voltage (Max) (V)	Ambient Temp (Max) (oC)	Ambient Temp (Min) (oC)	Internal RAM (KByte)	Other Peripherals	Bus Interface
66	1.5	3.3	0	70	8	DMA Controller	32-bit PCI, 8xx



External Bus Speed (Max) (MHz)	Security Encryption	Package Description
66	3DES, AES, ARC-4, DES, MD-4, MD-5, Public Key, RNG, SHA-1	MAPBGA252 21*21*0.8P1.27

▲ [Return to Top](#)

MPC184 Parametrics

## Documentation


### Application Note

ID and Description	Vendor ID	Format	Size K	Rev #	Date Last Modified	Order Availability
<a href="#">AN2576</a> MPC184 Descriptor Programmer's Guide_8xx View	FREESCALE	pdf	646	0	8/22/2003	
<a href="#">AN2492</a> MPC184 Descriptor Programmer's Guide--PCI View	FREESCALE	pdf	673	0	6/30/2003	


### Errata - [Click here for important errata information](#)

ID and Description	Vendor ID	Format	Size K	Rev #	Date Last Modified	Order Availability
<a href="#">MPC184CE</a> MPC184 Security Processor Device Errata	FREESCALE	pdf	505	7	10/28/2004	-





### Fact Sheets

ID and Description	Vendor ID	Format	Size K	Rev #	Date Last Modified	Order Availability
<a href="#">MPC184FACT</a> MPC184 Security Processor Fact Sheet	<a href="#">METROWERKS</a>	pdf	296	1	3/05/2003	




### Product Brief

ID and Description	Vendor ID	Format	Size K	Rev #	Date Last Modified	Order Availability
<a href="#">MPC184TS</a> MPC184 Security Processor	FREESCALE	pdf	224	1.1	2/18/2003	


### Reference Manual

ID and Description	Vendor ID	Format	Size K	Rev #	Date Last Modified	Order Availability
<a href="#">MPC1848XXHWRM</a> MPC184 8xx Mode Hardware Reference Manual	FREESCALE	pdf	398	2	3/25/2003	
<a href="#">MPC1848XXUM</a> MPC184 8xx Security Co-Processor Users Manual	FREESCALE	pdf	2100	1.1	5/25/2004	
<a href="#">MPC184PCIHWRM</a> MPC184 PCI Mode Hardware Reference Manual	FREESCALE	pdf	411	2.1	4/03/2003	
<a href="#">MPC184UM</a> MPC184 Security Co-Processor Users Manual PCI Interface	FREESCALE	pdf	3592	1.2	5/20/2004	



## Selector Guide

ID and Description	Vendor ID	Format	Size K	Rev #	Date Last Modified	Order Availability
<a href="#">SG1007</a> Network and Communications Processors Selector Guide	FREESCALE	pdf	189	0	1/01/2005	
<a href="#">SG2000CR</a> Application Selector Guide Index and Cross-Reference.	FREESCALE	pdf	128	6	1/01/2005	
<a href="#">SG2101</a> Regional Office Router	FREESCALE	pdf	123	4	1/01/2005	

## Users Guide

ID and Description	Vendor ID	Format	Size K	Rev #	Date Last Modified	Order Availability
<a href="#">MPC18XSWUG</a> MPC18XSWUG	FREESCALE	pdf	564	0	9/25/2003	

## White Paper

ID and Description	Vendor ID	Format	Size K	Rev #	Date Last Modified	Order Availability
<a href="#">PUBLICKEYPERFWP</a> Understanding Public-Key Performance	FREESCALE	pdf	56	0	2/10/2005	
<a href="#">SECURITYWP</a> Securing the Smart Network with Freescale Security Processors	FREESCALE	pdf	394	0.0	3/12/2002	

[▲ Return to Top](#)

MPC184 Design Tools

## Software

### Operating Systems

ID and Description	Vendor ID	Format	Size K	Rev #	Order Availability
<a href="#">ARA-MOT-82XX/8XX</a> Arabella Linux for Motorola 8xx/82xx Arabella Linux for Motorola 82xx/8xx processors is a full, commercial Linux distribution for the 82xx/8xx family of processors. Integrated support is included for the MPC180 Security Processors. Full reference designs are included.	<a href="#">ARABELLA</a>	-	-	-	-

[▲ Return to Top](#)

Applications

**Networking**

**SOHO**

[Regional Office Router](#)

[Wireless Gateway](#)

**Access**

[Remote Access Server](#)

**Applications**


[Regional Office Router](#)

[Wireless Gateway](#)

[Remote Access Server](#)

▲ [Return to Top](#)

Orderable Parts Information

Part Number	Package Description	Tape and Reel	<a href="#">Pb-Free Terminations</a>	<a href="#">Application/Qualification Tier</a>	Status	<a href="#">Budgetary</a>	Info	Order
						<a href="#">Price QTY 1000+ (\$US)</a>		
MPC184VFB	<a href="#">MAPBGA252 21*21*0.8P1.27</a>	No	No	COMMERCIAL	Available	-	<a href="#">more</a>	
MPC184VMB	<a href="#">MAPBGA252 21*21*0.8P1.27</a>	No	Yes	COMMERCIAL	Available	-	<a href="#">more</a>	-

**NOTE:**

- Not all orderable parts are offered through our online sampling program. For further assistance in selecting a similar part from within the program, please submit a [Request for a sample order advice](#).
- Refer to [Samples FAQ](#) for more information.
- Looking for an obsolete part? Check our [distributors' inventory](#)

▲ [Return to Top](#)

Related Links

- ▶ [Networking](#)
- ▶ [Wind River, HW Acceleration and Security Processor Support](#)
- ▶ [Zephyr Engineering, Inc.](#)

▲ [Return to Top](#)

