MM23SC8128RM

Flash Security Turbo Microcontroller Smart Card Chip With 1024 bit RSA & Maths Co-processor

08 September 2009

FEATURES

Short Introduction

GENERAL

- 0.25µm advanced FLASH technology.
- ISO7816 pin configuration
- Operating voltage of 2.7V-5.5V.
- Operating temperature -20^{0}C to 80^{0}C
- ESD protection > 6kV (HBM)
- External clock frequency of 1 MHz to 5 MHz
- Maximum internal clock frequency of 25Mhz
- Current consumption < 10mA at 10 Mhz.

SECURITY

- Hardware DES/Triple-DES coprocessor with countermeasures to any attack of power analysis or fault attempt
- 1024 bit RSA with non-CRT and CRT option
- Mathematical co-processors for complex mathematical operation of large integers
- Cyclic Redundancy Check (CRC) according to CCIT-16
- 32-bit Hardware Random Number Generator.
- Bus scrambler for byte-wise data address scrambling.
- Data memory encryption
- Clock desynchronisation option to vary power consumption
- Voltage, temperature and frequency sensor detection for anti-hacking
- Internal power on reset
- Signature Hashing Algorithm (SHA-1)
- Power Supply Low Voltage Detector to prevent a brown out condition in flash

PERIPHERALS

- UART ISO7816 with maximum of 115.2kbps, T=0 support.
- Two 16-bit timers
- Watchdog Timer

MEMORY

- 128K Bytes of FLASH non-volatile memory
  - 64K Bytes (512 Bytes per page) for program memory
  - 64K Bytes for data memory (64 Bytes per page)
- 4K Bytes of on-chip SRAM
- 512 Bytes and 64 Bytes SRAM buffers for Flash operation.
- CPU Internal data memory 256 Bytes SRAM.
- Data retention 10 years
- 500,000 write/erase cycles

SUPPORT

- NeoEvo integrated Software Development Kit and Emulator
- Application Note

GENERAL DESCRIPTION Short Introduction

MM23SC8128RM is a high performance enhanced 8-bit microcontroller smart card IC in 0.25um CMOS technology. The CPU can be clocked at 25Mhz as an option to speed up the processing time. MM23SC8128RM features significantly higher performance, high memory capacity and extremely low power consumption. Sleep mode is also available for low power applications.

MM23SC8128RM provides 64KBytes read-only flash memory and 64KBytes read/write flash memory with internal 256 Bytes Scratchpad RAM. An On-Chip Memory of 4K Bytes SRAM systems provides memory space for fast read/write access.

Communication protocol for the IC is according to IS07816-3 with UART modules to simplify IO management. An ETU counter is available for ETU management for IO communication. With a hardware implemented coprocessor for Mathematics operation, DES/3-DES, CRC, RSA and SHA, MM23SC8128RM is a powerful smart card IC enabling faster execution of cryptography execution and calculation. The 32 bit RNG co-processor provided in MM23SC8128RM ensures secured random number generation.

MM23SC8128RM is also equipped with power supply low voltage detector to prevent a brown out condition in flash memory area, data scrambling, clock desynchronisation option and memory encryption to provide highest security chip level.

PIN CONFIGURATION AND PIN NAME

Short Introduction

Pin configuration and pin name are shown in Figure 1 and Table 1.

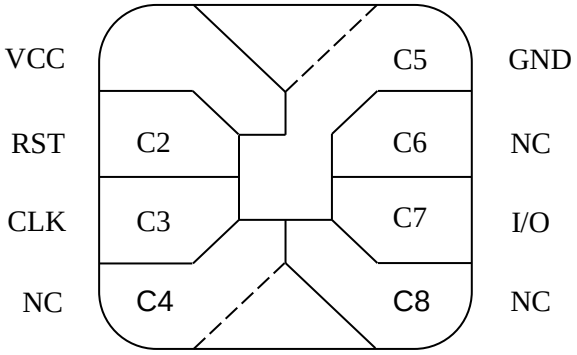

Figure 1: Pin Configuration

VCC	Power	C1
RST	Reset	C2
CLK	Clock Input	C3
NC	No Connection	C4
GND	Ground	C5
NC	No Connection	C6
I/O	Input/Output Connection	C7
NC	No Connection	C8

Table 1: Pin name

ARCHITECTURE OVERVIEW

Short Introduction

The MM23SC8128RM is based on the standard 8051 device which includes enhanced features of 8052, with improved speed and power consumption characteristics. It has the same instruction set as the 8051 family. The MM23SC8128RM executes all the standard 8051 instructions approximately 1.5 to 3 times faster in terms of number of clock cycles comparing to the traditional 8051 microcontroller. The block diagram is shown in Figure 2.

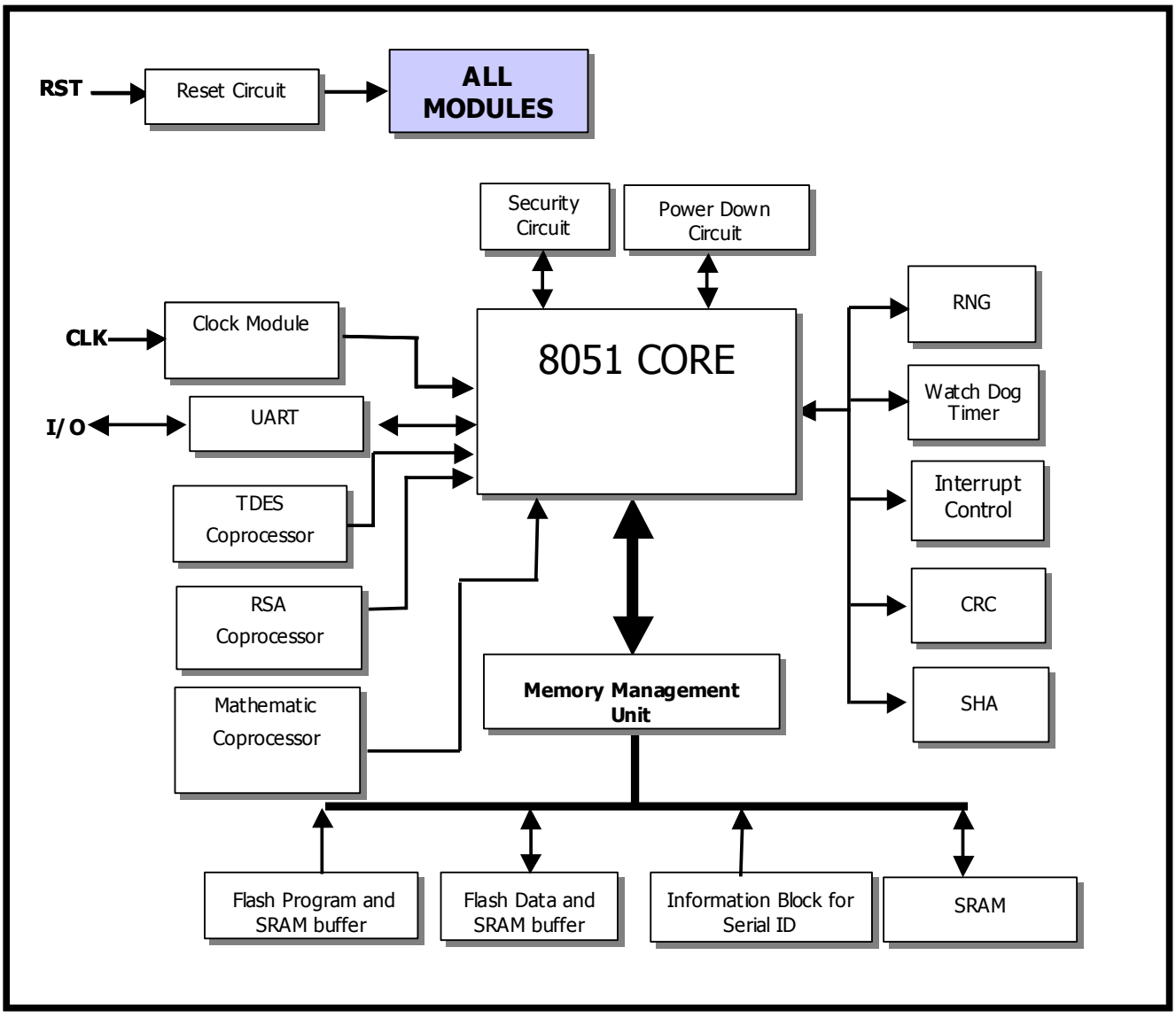

Figure 2: Block Diagram of MM23SC8128RM

MEMORY BLOCK DIAGRAM

Short Introduction

The Flash Program Memory and the Flash Data Memory start from 0000H to FFFFH. Refer to Figure 3 below.

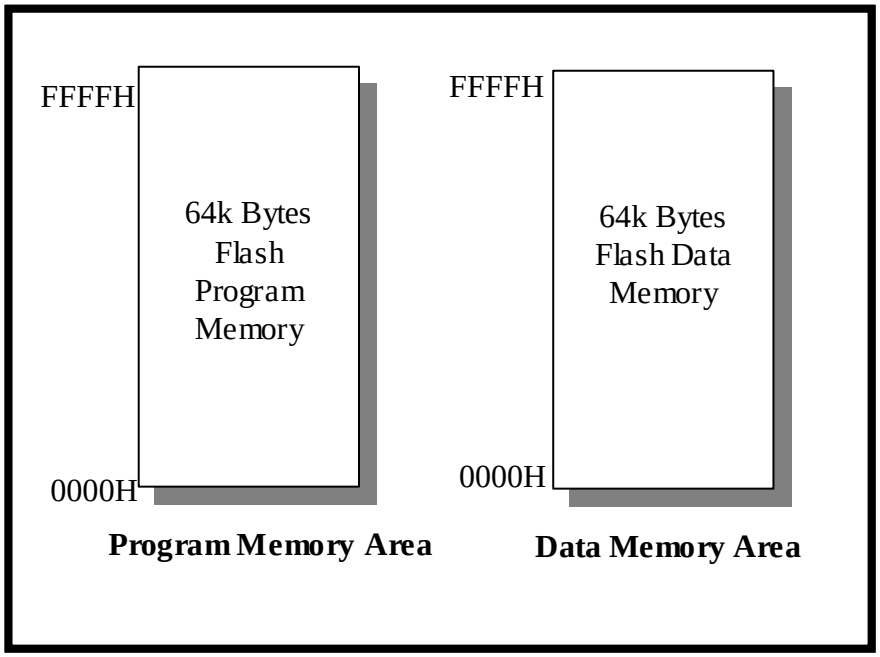

Figure 3: Flash Program and Data Memory Area

32-BIT RANDOM NUMBER GENERATOR PROCESSOR

The MM23SC8128RM provides an RNG processor that output 32 bits of random seeds at every warm or cold reset and whenever seed generation instruction is driven. The random output bit can be used for Initialization Vector(IV) generation, or to be used in others cryptographic application.

ELEMENTARY TIME UNIT (ETU) COUNTER

Short Introduction

ETU counter is to serve as a timer, and to serve as a bridge for data transfer between reader and the MCU. ETU counter is used to count the ETU while the code is running. A typical smartcard IO operation, APDU is issued by the reader to the card and Status Word is issued by the card indicating that the operation is completed.

The ETU counter comes into the picture where the operation requires a long time between the APDU and the Status Word. A wait/null byte after APDU is sent out to the reader. As defined in ISO7816-3, the null byte shall acknowledge the reader that the process is still ongoing so that the reader will not send a timeout error. In MM23SC8128RM, the delay between the leading edges of two consecutive characters sent by the card can be configured.

UART-7816

The MM23SC8128RM UART-7816 operation has 6 major modules:

- UART-7816 controller and 8051 interface. These modules connect the UART-7816 operation to the chip via the 8051 Special Function Registers (SFRs) selection. The 8051 interface is running at 8051 clock.
- Baud Rate Generator selects the Baud Rate as defined in ISO-7816.
- Receiver for T0 or T1 operation
- Transmitter for T0 or T1 operation
- FIFO for Receiver
- FIFO for Transmitter

CRC COPROCESSOR

The MM23SC8128RM has a Cyclic Redundancy Code (CRC) co processor that will generate a 16-bit checksum when using ISO3309 ($x^{16}+x^{12}+x^5+1$). The MM23SC8128RM supports two modes of CRC which are CCITT V.41 and HDLC X25.

TDES COPROCESSOR

The MM23SC8128RM provides a TDES coprocessor which is based on Data Encryption Standard published by Federal Information Processing Standards Publication (FIPS 46-3). Encryption and decryption are implemented in the same core to provide flexibility to system integration. ECB mode is supported for cryptographic system or security application. The TDES Engine is an on-chip peripheral, improving system performance by supporting rapid encryption and decryption of data blocks. It can perform the Data Encryption Standard, DES, algorithm in single DES and triple DES mode.

The TDES coprocessor internal design is also equipped with a countermeasures to any attack of power analysis or fault attempt to guess the key.

MATH-COPROCESSOR

Math-Coprocessor consists of several modules:

I) Multiplication
II) Addition
III) Subtraction
IV) Comparator (a > b)
V) Shift Left 1-bit
VI) Shift Right 1-bit
VII) Zero Reduction

It is capable of performing operation on integers bits 32, 64, 128, 256, 512, 1024. This will enable mathematic operations on large integer bits.

1024-BIT RSA PUBLIC-KEY CRYPTOGRAPHIC COPROCESSOR

The MM23SC8128RM RSA crypto co-processor has an option to choose CRT (Chinese Remainder Theorem). The co-processor enables faster execution of RSA calculation.

The performance of RSA operation is summarized in the following table:

Table 18: Performance of various RSA operations

Exponent	No.of '1'	No. of '0'	Modulus	Computation Time @ 25 MHz external clock
1024 bit [2]	512	512	1024 bit	250ms (Non-CRT)
1024 bit [2]	512	512	1024 bit	150ms (CRT)

[1] The public key $e = 2^{16} + 1 = 65537$ is used.

[2] Average case, 1024-bit exponent, 50% '1', 50% '0' in binary representation.

SHA COPROCESSOR

The MM23SC8128RM is equipped with SHA coprocessor. It follows Digital Signature Standard, NIST for ensuring security of Digital Signature Algorithm (DSA). When a message of any length < 2^{512} bits is entered as input, the SHA produces a 160-bit

output called a message digest. The message digest is then entered as input to the DSA. This engine computes the signature for the message. Signing the message digest rather than the message often improve the efficiency of the process. The same message should be obtained by the verifier of the signature when the received version of the message is used as input to SHA.

The MMM23SC8128RM SHA coprocessor is secured because it is designed to be computationally infeasible for hacker to recover a message corresponding to a given message digest, or to find two different messages which produces the same message digest.

ORDERING INFORMATION

Short Introduction

Order Part Number	Package
MM23SC8128RM – SW	Sorted Wafer
MM23SC8128RM – DW	Dice in waffle pack after backgrinding to 8 mil.
MM23SC8128RM – SR	Sorted wafers on a ring
MM23SC8128RM – TR	Modules in tape and reel

Edition 2009

Published by Malaysia Microelectronic Solutions Sdn. Bhd. (*My-MS*)

Attention please!

The information herein is given to describe certain components and shall not be considered as warranted characteristics. Terms of delivery and rights to technical change reserved.

We hereby disclaim any and all warranties, including but not limited to warranties of non-infringement, regarding circuits, descriptions and charts stated herein.

Information
For further information on technology, delivery terms and conditions and prices please contact My-MS directly.

Warnings
My-MS' products are not authorized for use as critical components in life support devices or systems.

Malaysia Microelectronic Solutions
Suite B-03-06, 3rd Floor, Block B,
No. 9 Jalan 11/16, Off Jalan Damansara,
Phileo Damansara 1, 46350 Petaling Jaya,
Selangor Darul Ehsan,Malaysia.
Tel: +603 8318 1011
Fax: +603 8318 1012
URL: http://www.my-ms.com