

Features

General

- 0.5 μ Process Technology
- Industry-standard M68HC05 Instruction Set, including: 8 x 8 bits Unsigned Multiply Instruction, True Bit Manipulation, Memory-mapped I/O
- Operating Voltage: 3.0V \pm 10% or 5.0V \pm 10%
- Meets GSM 11.11 & 11.12 Specifications
- 5.0 MHz Maximum Internal Bus Frequency at 3.0V and 5.0V
- ESD Protection to \pm 4000V
- Bond Pad Layout Conforming to ISO Standard ISO 7816/2
- External Maskable Interrupt on ISO Standard I/O Port (PA0)
- Power-saving WAIT and Very Low Power STOP Modes
- Power-up Detection
- Available as Sawn or Unsawn Wafers or in Industry-standard Packages and Modules

EEPROM

- 8128 Bytes of On-chip User EEPROM, plus 64 Security Bytes
- 1 to 64-byte Write/Program/Erase
- 1 ms Program Time, 1 ms Erase Time
- 10 Years Data Retention
- Typically more than 1,000,000 Write/Erase Cycles
- On-chip Charge Pump for EEPROM Programming Driven by an Internal Oscillator

RAM and ROM

- 32752 Bytes of On-chip User ROM plus 16 Bytes Reserved for Vectors
- 1024 Bytes of On-chip RAM with Security Wipe on Selected Areas

Peripherals

- Single Bidirectional I/O Line (1-bit ISO 7816/3 Standard I/O Port)
- Time Base Circuitry (with Preset and Maskable Interrupt Capabilities)
- Watchdog Capability
- Hardware DES Module (Capable of Single Encryption or Decryption in 16 Clock Cycles)
- CRC Module (allowing generation of Checksums (ISO/IEC 3309))
- Random Number Generator

Security

- Dedicated Hardware to Resist Power Analysis Attacks
- Featureless ROM
- Low and High Voltage Monitors
- Low and High Temperature Monitors
- Low Frequency Monitor
- High Frequency Filter/Monitor
- Advanced Physical Barrier to Enhance Tamper Resistance
- Illegal Address Reset
- Illegal Opcode Reset
- Memory Partitioning with Address Lockout Reset
- Scrambling Logic
- Tamper Monitor
- Physical Removal of Test Mode when Testing is Complete

Development Tools

- Hardware Emulation Module (for the Motorola MMDS05 Development System)
- Software Simulator based on HIWARE's HI-WAVE Product



8-bit Secure Microcontroller with 8K EEPROM and Advanced Security Features

AT05SC3208R

Preliminary

Summary

Rev. 1505BS-04/00



Note: This is a summary document. A complete document is available under NDA. For more information, please contact your local Atmel sales office.

Description

The AT05SC3208R is a new member of Atmel's AT05SC family of single chip microcontrollers. Designed specifically for embedded conditional access systems and other security conscious systems, these devices are based on the industry-standard M68HC05 low-power core and its instruction set.

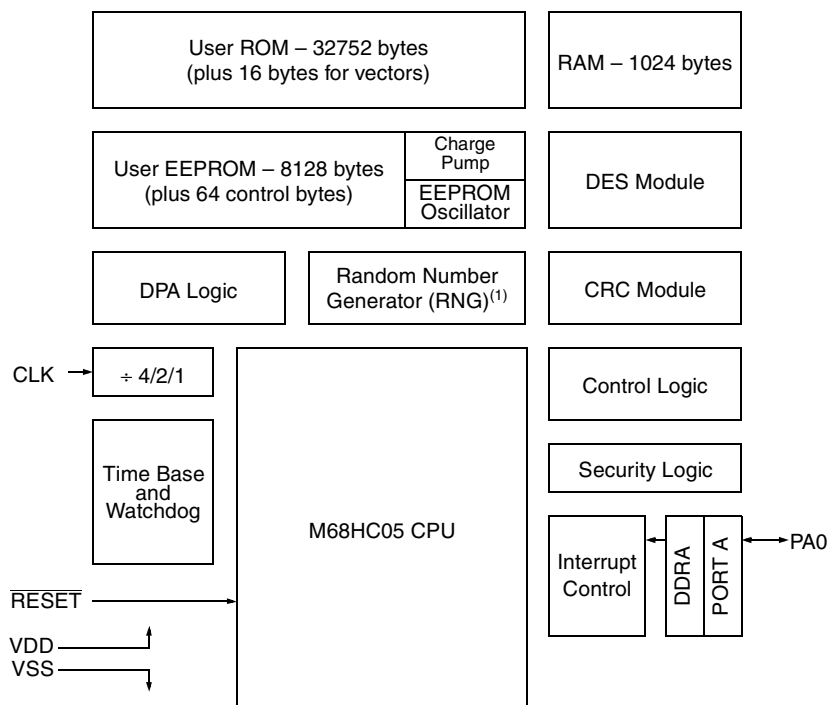
The AT05SC3208R is designed to give a high level of protection against physical and power analysis attacks, and includes hardware features to assist in protecting against SPA and DPA attacks. On-board DES, CRC and RNG

modules are provided to assist in the design of high-security applications.

On-board memory comprises 32K bytes of ROM, 1K bytes of RAM and 8K bytes of EEPROM. The EEPROM features 64-byte write, 1 ms program time, 1 ms erase time, typically more than 1,000,000 write/erase cycles, and greater than 10 years data retention.

Application areas for the AT05SC3208R include Finance, GSM Mobile Phones and Set-top Boxes.

Block Diagram



Note: 1. A sampling/smoothing algorithm MUST be used in conjunction with the RNG to obtain statistically random results across all operating conditions.



© Atmel Corporation 2000.

Atmel Corporation makes no warranty for the use of its products, other than those expressly contained in the Company's standard warranty which is detailed in Atmel's Terms and Conditions located on the Company's web site. The Company assumes no responsibility for any errors which may appear in this document, reserves the right to change devices or specifications detailed herein at any time without notice, and does not make any commitment to update the information contained herein. No licenses to patents or other intellectual property of

Atmel are granted by the Company in connection with the sale of Atmel products, expressly or by implication. Atmel's products are not authorized for use as critical components in life support devices or systems.

Atmel Headquarters, 2325 Orchard Parkway, San Jose, CA 95131, TEL (408) 441-0311, FAX (408) 487-2600
 Atmel Colorado Springs, 1150 E. Cheyenne Mtn. Blvd., Colorado Springs, CO 80906, TEL (719) 576-3300, FAX (719) 540-1759
 Atmel Rousset, Zone Industrielle, 13106 Rousset Cedex, France, TEL (33) 4-4253-6000, FAX (33) 4-4253-6001
 Atmel Smart Card ICs, Scottish Enterprise Technology Park, East Kilbride, Scotland G75 0QR, TEL (44) 1355-357000, FAX (44) 1355-242743

Marks bearing ® and/or ™ are registered trademarks and trademarks of Atmel Corporation.

Terms and product names in this document may be trademarks of others.



Printed on recycled paper.

1505BS-04/00/xM