



Secure Microcontroller

AT90SC320288RCT Summary

Features

General

- High-performance, Low-power 8/16-Bit RISC Architecture
 - 135 Powerful Instructions (Most Executed in a Single Clock Cycle)
- Low Power Idle and Power-down Modes
- Bond Pad Locations Conforming to ISO 7816-2
- ESD Protection to $\pm 6000V$
- Operating Ranges: 2.7 to 5.5V
- Compliant with GSM, 3GPP and EMV 2000 Specifications, PC Industry Compatible
- Available in Wafers, Modules, and Industry-standard Packages

Memory

- 320K Bytes of ROM Program Memory
- 288K Bytes of EEPROM, Including 128 OTP Bytes and 384 Bit-addressable Bytes
 - 1 to 128-byte Program / Erase
 - 1.25ms Program / 1.25ms Erase
 - Typically 500,000 Write/Erase Cycles at a Temperature of 25°C
 - 10 Years Data Retention
 - EEPROM Erase only mode
 - Write EEPROM with or without autoerase
- 8K bytes RAM Memory (6K bytes of CPU RAM, 2K bytes of Ad-X™ RAM, shared with the CPU core)
- 32K Bytes of ROM Dedicated to Inside's Crypto-library

Peripherals

- Two I/O Ports
 - Configurable to Support Communication Protocols, Including ISO7816-3 and 2-wire protocols
- One ISO 7816 Controller
 - Up to 625 Kbps at 5 MHz
 - Compliant with T=0 and T=1 Protocols
- Serial Peripheral Interface (SPI) Controller (up to 12 MHz)
- Programmable Internal Oscillator
 - Up to 20 MHz on ROM
 - Up to 40 MHz for Cryptographic Accelerator
- Two 16-bit Timers
- Random Number Generator (RNG)
- 2-level, 8-vector Interrupt Controller
- Hardware DES and Triple DES DPA/DEMA Resistant
- Checksum Accelerator
- CRC16 & 32 Engine (Compliant with ISO/IEC 3309)
- 32-Bit Cryptographic Accelerator (Ad-X for Public Key Operations)
 - RSA, DSA, ECC, Diffie-Hellman

Security

- Dedicated Hardware for Protection Against SPA/DPA/SEMA/DEMA Attacks
- Advanced Protection Against Physical Attack, Including Active Shield
- Environmental Protection Systems
- Voltage Monitor
- Frequency Monitor
- Temperature Monitor
- Light Protection
- Secure Memory Management/Access Protection (Supervisor Mode)

Certification targeted

- CC EAL4+
- VISA
- CAST
- FIPS

Description

The AT90SC320288RCT is a low-power, high-performance, 8/16-bit microcontroller with ROM program memory, EEPROM memory, based on the RISC architecture.

By executing powerful instructions in a single clock cycle, the AT90SC320288RCT achieves throughputs close to 1 MIPS per MHz. Its Harvard architecture includes 32 general-purpose working registers directly connected to the ALU, allowing two independent registers to be accessed in one single instruction executed in one clock cycle.

The ability to map the EEPROM in the code space allows parts of the program memory to be reprogrammed in-system. This technology combined with the versatile 8/16-bit CPU on a monolithic chip provides a highly flexible and cost-effective solution to many smart card applications. The AT90SC320288RCT benefits of advanced EEPROM functions (XP Mode), but can also be configured to offer compatibility with previous product generations (e.g. AT90SC25672R or AT90SC19236R)

Development Tools

- Voyager Emulation Platform (ATV4) to Support Software Development
- IAR Embedded Workbench® V3.20c Debugger or Atmel's AVR Studio® Version 4.07 or Above
- Software Libraries and Application Notes

The cryptographic accelerator, running with the RISC core, featured in the AT90SC320288RCT series is the new Ad-X. It is based on a 32-bit multiplier-accumulator architecture which is designed to perform fast encryption and authentication functions. This enables fast computation and low-power operation. The controlling firmware is located either in the dedicated ROM memory (Inside's cryptolibrary supports standard finite field arithmetic functions including RSA, DSA, DH and ECC) or in the ROM program memory (customer specific).

Additional security features include power and frequency protection logic, logical scrambling on program data and addresses, Power Analysis countermeasures and memory accesses controlled by a supervisor mode.

Figure 1 shows a block diagram of the AT90SC320288RCT

Figure 1 AT90SC320288RCT Enhanced RISC Architecture

