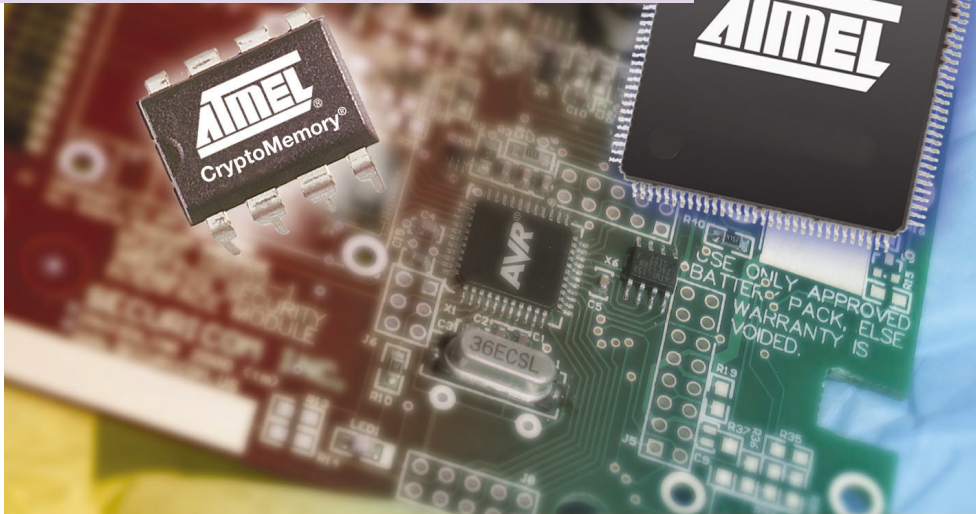# AT88SC0104C to AT88SC25616C

FAMILY OF CRYPTOMEMORY® SECURE SERIAL ICS

The new CryptoMemory family of devices in plastic packages provides secure serial EEPROM storage for sensitive information within an embedded system.

Key Features

- A Family of Devices with User Memories from 1 Kbit to 256 Kbits: 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K
- Symmetrical Dynamic Mutual Authentication with 64-bit Cryptographic Keys
- Encrypted Passwords with Attempts Counters
- Stream Encryption Ensures Data Privacy
- AVR®-based Interface Software Available for Easy Implementation
- 1.5 MHz Compatible 2-wire Serial Interface for Fast Operation
- Standard 8-lead SOIC, PDIP and LAP Packages Available, Using the Same Pinout as Atmel's AT24Cxx 2-wire Serial EEPROMs

Applications

- Subscriber Systems (set top boxes)
- Access Control Systems
- Subassembly Authentication
- Removable Storage Devices
- Networked Systems

CryptoMemory Cryptographic Security ICs offer a low cost, high security solution for any embedded application requiring data protection. A proprietary cryptographic algorithm encrypts data, passwords and checksums, providing a secure place for storage of sensitive information within a system. With its tamper detection circuits, this information remains safe even under attack. Whether it is factory configuration data, user preference data or encryption keys that need to be protected, Atmel's CryptoMemory offers a secure solution.

Security

The device includes a proprietary algorithm for encrypting data and passwords and providing a MAC for read and write operations. Access to data stored in the device is also protected by an authentication routine. Various security options are available, including four unique key sets for authentication and eight unique password sets. Encryption is performed using a new session key each time the device is accessed. The setting of security options along with keys and passwords is performed by simply writing to a configuration zone in the memory when initial data is loaded into the device. Atmel's CryptoMemory family was developed after many years of designing chips for the smart card marketplace, a market where security is key. The same techniques used to keep information safe from attack in smart cards is now available to the embedded market.

Communications

CryptoMemory utilizes a common 2-wire serial interface for easy implementation with any microcontroller. Running at up to 1.5 MHz, this synchronous communications interface ensures fast operation in any system. With its set of 15 commands, CryptoMemory offers the flexibility to use any or all of its security features to protect up to 256 Kbits of information.

Implementation

Hardware implementation is easy: CryptoMemory uses the same familiar pinout as Atmel's AT24Cxx 2-Wire Serial EEPROMs and is available in standard plastic packages. All memory densities of CryptoMemory are available in space-saving SOIC and LAP packages as well as PDIPs. Software implementation requires the CryptoMemory command set and cryptographic algorithm to be ported into your system's controller or logic. Full documentation is available under NDA; for AVR users, a Software Development Toolkit (AT88SC25616C-SDT) is available for easy integration of CryptoMemory into your system.

Packaging

CryptoMemory circuits are available in standard plastic packages (SOIC, PDIP, LAP) for PC board assembly with the same pinout as Atmel's AT24Cxx serial EEPROM family.
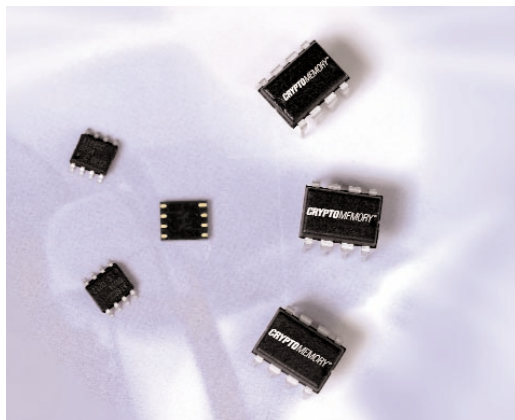
Atmel contact: cryptomemory@atmel.com