AT88SC0104C to AT88SC25616C

FAMILY OF CRYPTOMEMORY™ SECURITY CHIPS

PURPOSE

Atmel's CryptoMemory is a new Secure Memory family of products with memory densities from 1 Kbit (AT88SC0104C) to 256 Kbits (AT88SC25616C) for smart card and embedded applications.

This new family of secure circuits makes available to the industry a low cost, high security chip solution that fills the void between plain serial EEPROM memories and microprocessors. Memory densities from 1 Kbit to 256 Kbits are available now.

AT88SC0104C to AT88SC25616C

This is the only Secure Memory family of devices in the industry with mutual authentication between card and reader, and data encryption for both synchronous and asynchronous protocols.

FEATURES

- A Family of Devices with User Memories from 1 Kbit to 256 Kbits (1, 2, 4, 8, 16, 32, 64, 128, 256)
- Symmetrical Dynamic Mutual Authentication, 64-bit Cryptographic Key to Authenticate Reader and Card
- Encrypted Passwords with Attempts Counters, Encrypted with a Different Key for Each Usage
- Stream Encryption Ensures Data Privacy
- Read and Write Encrypted Checksum, Guaranteeing Data Integrity and Authenticity of the Source
- Anti-tearing, Avoids Data Corruption or Recovers Data in Case of Power Loss
- Dual Communication Protocol, ISO 7816-3 Asynchronous T=0 and Synchronous Two-wire
- Can Be Used in Virtually Any Reader
- Devices 32 Kbits and Larger Support ISO 7816-3 PPS Exchange for Communication Speeds up to 153,600 Band
- 2.7V to 5.5V Operation

SECURITY

The device includes a random generator and a proprietary algorithm similar to DES for encrypting data, passwords and providing MAC for read and write operations, thus providing data integrity and certification of data origin. Each device is differentiated from all others after personalization through a unique identification number and set of secret keys. The device secret keys are issued from the application secret keys using an encryption algorithm such as DES, 3DES, AES, etc., which is chosen by the issuer. This function is performed outside of the device.

Corporate Headquarters
2325 Orchard Parkway
San Jose, CA 95131
TEL (408) 441-0311
FAX (408) 487-2600

Europe
Atmel Sarl
Route des Arsenaux 41
Case Postale 80
CH-1705 Fribourg
Switzerland
TEL (41) 26-426-5555
FAX (41) 26-426-5500

Asia
Room 1219
Chinachem Golden Plaza
77 Mody Road Tsimshatsui
East Kowloon
Hong Kong
TEL (852) 27219778
FAX (852) 27221369

Japan
9F, Tonetsu Shinkawa Bldg.
1-24-8 Shinkawa
Chuo-ku, Tokyo 104-0033
Japan
TEL (81) 3-3523-3551
FAX (81) 3-3523-7581

Atmel Operations
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

e-mail
literature@atmel.com

Web Site
http://www.atmel.com

ADVANTAGES

CryptoMemory has many features that make it the only product on the market that supplies low cost and high security solutions:

- Full family available, allowing system integrator to switch memory density as application needs increase without changing application software
- No operating system needed; easy to program, allowing faster time to market
- More secure and flexible than small microprocessors (<16 Kbytes ROM)
- Savings up to 50% compared to microprocessor implementation
- Add security to your serial EEPROM embedded applications for just pennies more

APPLICATIONS

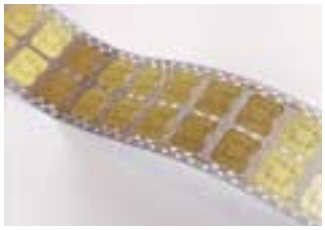
CryptoMemory can be used in smart cards or embedded applications:

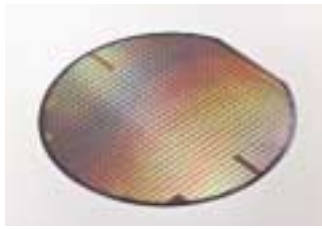
- Smart Card Applications: ID cards, driving licenses, insurance cards, access control, administrative cards, campus cards, voting machines, e-purse, loyalty, energy meters, parking meters, transaction records and multi applications.
- Embedded Applications: Secure data on printed circuit boards for computers, networking systems, PDAs, electronic equipment, automotive, telecommunications and industrial. Storing secret keys and authentication of OEM subassemblies within a system, i.e. removable storage devices, automotive piece parts, and replaceable components.

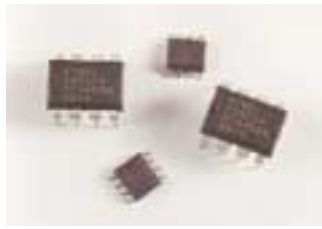
PACKAGING

CryptoMemory circuits can be packaged to meet customer needs:

- Wafer form, thinned to customer thickness specifications
- Smart Card Modules compliant to ISO 7816-2
- Plastic packages (SOIC, PDIP, LAP) for PC board assembly, same pinout as Atmel's AT24Cxx Serial EEPROM family







DEVELOPMENT KIT

Atmel offers a Development Kit (AT88SC25616C-DK) for the CryptoMemory family to assist in writing asynchronous applications for any density device from 1 Kbit to 256 Kbits. The kit is sold under NDA and enables the developer to write applications utilizing the full CryptoMemory feature set. The kit includes:

- A PC/SC compliant card reader
- Sample CryptoMemory cards
- API and documentation
- Sample program and tutorial

Additional information is available on our web site, through our sales offices or by emailing us at securememories@atmel.com.

2044B/10/02/13.5K