ATMEL WHITE PAPER

Understanding CryptoMemory â

The World's Only Secure Serial EEPROM

By Dale Anderson, Applications Engineer

Summary

CryptoMemory is Atmel's secure serial EEPROM solution with the same pinout as the AT24Cxxx series, making it easy to upgrade from an open EEPROM to a secure solution for embedded applications. With its dual communications protocol, CryptoMemory also provides secure solutions for the smart card market. This paper describes the four security levels of CryptoMemory and how to implement them in a system.

Atmel Corporation • 2325 Orchard Parkway • San Jose, CA 95131
TEL (408) 441-0311 • FAX (408) 487-2600 • Web Site: *http://www.atmel.com*

CryptoMemory, Atmel's most advanced secure memory product, is a family of serial EEPROM devices available in capacities up to 256K bits with advanced security features, including data encryption/decryption. With trusted EEPROM technology as its core, this secure stand-alone memory is based on Atmel's years of experience in the smart card and security markets.

A wide variety of markets require secure serial EEPROM. CryptoMemory was first introduced in the smart card marketplace, offering an easy-to-implement secure solution that communicates with standard card readers. One card has the capability to manage multiple applications. In an office or campus environment, CryptoMemory can be used as an ID card for access control and as a stored value card for cafeteria, parking or other services. CryptoMemory can also be used as an electronic key to unlock system features.

CryptoMemory is designed to keep contents secure, whether operating in a system or removed from the board and sitting in the hacker's lab. Information about the system, about the user, or about a component of the system can easily be stored in this secure nonvolatile device. CryptoMemory provides a secure location for a manufacturer to store information not accessible by the user and can protect specific user data from other authorized applications. It also provides a unique and secure ID for removable components to control use in a system and prevent counterfeiting.

To create the CryptoMemory device, Atmel started with reliable EEPROM technology, which is structured in such a way that it is almost impossible to physically determine memory contents in an unauthorized die-level attack. EEPROM memory is divided into zones or sectors, giving CryptoMemory the ability to isolate data for different uses or applications on one chip. Access to the EEPROM is only through the security logic that surrounds the memory. This logic is hard-wired and cannot be modified or tampered with in an attempt to bypass any of the security features. Each zone of the memory can be independently configured to operate as full read/write, read-only, or program-only memory; or can operate in a special write-lock mode that allows locking the memory in smaller sections. These memory features provide flexibility to the application developer, while the configurable security options make CryptoMemory a desirable secure storage device.

Different Levels of Security

Each zone of the memory can be independently configured to require different levels of security screening before its contents can be accessed.

First Option: No Security

With this option, one or more zones are set up with open access for data that does not require protection.

Second Option: Password Protection

A password must be successfully presented before access is granted to the protected memory zone. Only four incorrect attempts are allowed before that password and the protected zone are locked permanently.

Third Option: Authentication

Increasing the security another level, the authentication option protects one or more memory zones. In this security level, 64-bit cryptograms are exchanged; independent calculations are performed for a dual authentication between CryptoMemory and the host logic. Incorrect attempts are limited, and access is granted to the protected memory zone only after successful calculations.

Fourth Option: Data Encryption and MACs

The highest level of security utilizes data encryption and message authentication codes (MACs). To use encryption, authentication must be successfully performed first. With each successful authentication, a new 64-bit session key is generated. This key is used for subsequent encrypted read and write operations. When a memory zone is configured to require encryption, all data exchanges will be encrypted. A MAC may be requested to further validate data read from the device, and a MAC is required for each data string to be written to CryptoMemory.

Tamper Protection

Protection provided by CryptoMemory doesn't stop with the features built into logic. A hacker is likely to operate a device outside its normal conditions to try and bypass the logic and gain access to the memory contents. Tamper protection circuits have been added to CryptoMemory to stop hackers. These circuits will detect operations outside the defined limits and will safely shut down the device, preventing all access to its contents.

Implementing CryptoMemory

The first step in implementing CryptoMemory is to determine which memory and security features are needed. Then determine if data will be stored for different applications or will require different security levels, because the security settings are defined for each zone of memory. Once the data configuration and security settings have been defined on paper, initialize the CryptoMemory device.

The memory and security feature settings are stored in a special configuration zone of the EEPROM. Each zone has its own access register in this configuration zone. By programming this access register, the selected memory and security features for each memory zone are set. When two or more zones share the same features, the access registers are programmed the same. Multiple password and key sets are available for passwords authentication or encryption. The password or key set is also programmed into the access register for each EEPROM zone. Then the actual values for passwords and keys are programmed into specific locations of the configuration zone. Programming the configuration zone is as simple as programming an EEPROM. Once all values are written, a sequence of fuses is set, using a special write command to permanently lock the configuration zone. CryptoMemory is now ready for field use with its user-defined security settings and keys. After the configuration zone programming is completed, CryptoMemory becomes a unique security device customized to each application – from low security to high security or with several security levels on the same device.

To make using CryptoMemory easier, two well-known communication protocols are supported. For smart card applications, the ISO 7816-3 T=0 asynchronous protocol allows

CryptoMemory to interface with any standard PC/SC reader in the market today. For embedded applications, the popular 2-wire serial interface is the same interface used on serial EEPROMs. The 4-byte commands used to operate CryptoMemory are simple and straightforward, whether setting the memory zone, reading and writing, or enabling authentication and encryption.

Atmel's CryptoMemory family includes nine devices, from the 1-Kbit AT88SC0104C to the 256-Kbit AT88SC25616C. All devices share the same architecture, security features and communications protocol, allowing users to easily switch between members of the family as memory needs dictate. CryptoMemory offers many options for secure serial EEPROM with data encryption and other advanced security features. For even more options, Atmel's new CryptoRF™ offers all the features of CryptoMemory with a 13.56 MHz RF interface compliant to ISO 14443-B.

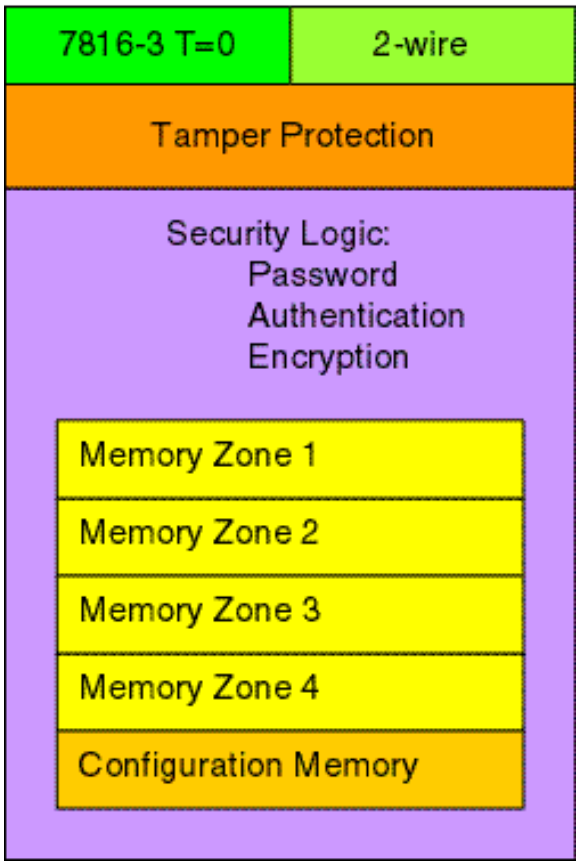

Figure 1. The physical layers of CryptoMemory. Note how the logic surrounds the memory, and tamper protection resides between communication protocols and the logic.

About Atmel

Founded in 1984, Atmel Corporation is headquartered in San Jose, California with manufacturing facilities in North America and Europe. Atmel designs, manufactures and markets worldwide, advanced logic, mixed-signal, nonvolatile memory and RF semiconductors. Atmel is also a leading provider of system-level integration semiconductor solutions using CMOS, BiCMOS, SiGe, and high-voltage BCDMOS process technologies.

Further information can be obtained from Atmel's Web site at www.atmel.com.

Contact: Dale Anderson, Applications Engineer, Atmel Corp., 1150 E. Cheyenne Mtn. Blvd., Colorado Springs, CO 80906; 179-540-0000; danderson@atmel.com