ATMEL WHITE PAPER

CRYPTOMEMORY – POWERFUL SECURITY AT LOW COST

By Eustace Asanghanwa, Crypto & RF Memory Applications

Summary

Many systems and products have the need to combat piracy or securely store information. Secure Microcontrollers satisfy this need at a high cost characterized by presence of unneeded features. CryptoMemory® provides a low-cost alternative solution that focuses mainly on security. www.cryptomemory.com

Table of Contents

Problem and Motivation

The International Chamber of Commerce (ICC) reported counterfeit and piracy activities valued at US$1.54 Billion in 2005 from just 1,479 incidences in 80 countries in its Global Counterfeit & Piracy Report for 2005. Included in these activities are US$289 Million worth of seizures in the US from 402 incidences, $516 seizures from 240 incidences in UK, $95 Million from 12 incidences in Germany, $137 Million from 24 incidences in Russia and $21 Million from 18 incidences in South Africa. Industries with top counterfeit seizures were Entertainment & Software with seizures valued at $695 Million, Clothing & Accessories at $283 Million, Cigarettes and Tobacco at $193 Million, Drugs & Medical at $61 Million, and Industrial Goods at $56 Million. The most seized brands were Microsoft, Louis Vuitton, Nike, Gucci, and Addidas. The variety of products seized is wide to include software IP, consumables, medical, cosmetics, and food, tobacco & alcohol. Top 4 countries traced to distribution and manufacturing sources were China, Nigeria, Turkey, and Taiwan for products manufactured all over the world. This and similar reports clearly demonstrate all products are susceptible to counterfeits irrespective of product type, markets, or geographic location where the authentic products are manufactured, and that the manufacturability of counterfeit products is possible anywhere in the world. More recent data indicates the problem is not improving, for instance, ICC reports 11% increase in IP counterfeit activities in first quarter of 2006 compared to first quarter of 2005. With such a trend, one cannot ignore the problem and most importantly the cost of counterfeit.

The cost of counterfeit is enormous. The cost is comprised subcategories to include loss of market share, brand erosion, bad will, liability from low quality fakes, and support costs for the non-authentic products. Avoiding counterfeit costs entails protecting your product from counterfeit. This entails understanding counterfeit itself. For the pharmaceutical industry, the US Food and Drug Administration (FDA) under Federal Law [21 USC 321(g)(2)] defines a counterfeit drug product as "a drug sold under a product name, without proper authorization, that is represented, labeled, packaged in a manner that suggests it is an authentic approved product". This definition applies equally well to every counterfeit product in the market. Any fake product packaged right will pass for the authentic product. The problem of counterfeit, therefore, becomes that of product labeling and identification.

Existing Product Labeling Solutions and Corresponding Anti-Counterfeiting Resistance

Good anti-counterfeit measures involve creating high barrier to copying identification information of authentic products. This involves labeling authentic products with identification features that are extremely difficult to duplicate. Traditional product labeling techniques, which include text labeling, barcodes, and graphical markings or symbols, have no such features hence render products susceptible to counterfeiting.

The shortcomings of traditional product labeling techniques has let to novelty labeling methods which, though offer slightly higher resistance to cloning, do not solve the problem. These methods include embedding an IC memory into the product and digitally encoding the content with the product information. Some of these memories have wireless interfaces and get used as in widely recognized Radio Frequency Identification (RFID). The improve barrier to cloning, some of these memories come with password protection, and some

vendors even encrypt the label information to embed in the memory. The fact of the matter is that passwords are easily attacked either through brut force or message replay techniques. Encrypting the labels do not offer any additional barrier to cloning, as the encrypted label, even if encrypted using strong algorithms with biometrically enhanced information like fingerprints, can still be digitally duplicated and populated in billions of other embedded memories. The proper solution to product counterfeit, therefore, requires denial of access to the labeling information embedded in the product except by an authentic source. This requires the use of authentication technology. Authentication requires that the party (host) attempting to access the product label first authenticates itself before being granted access. If the host happens to be a counterfeiter, it will not be able to authenticate itself, will be denied access, and so cannot duplicate labeling information it does not possess. Table 1 summarizes various labeling techniques and protection strengths.

Table 1. Existing Labeling Technology

Existing Solutions	Counterfeit Protection	Data Protection	Offered By
Paper labels	None. Can be cloned	None	Completion
2-D Bar Codes	None. Can be cloned	None	Completion
Embedded Memory/Tags	None. Can be cloned	None	Completion
Encrypted Message in Memory/Tags with password	Weak. Can be cloned	Weak	Completion
Security Generated with the Device	**STRONG**	**STRONG**	**CRYPTOMEMORY**

Given the fact that an authentic host requires proper reader hardware to access the label information, one may be tempted to question the practicality of such a solution. For instance, if one is only going to purchase a single Louis Vuitton handbag in a year, does this single transaction justify purchasing a label reader? Probably not, however, a store that stakes in reputation in providing authentic products will find buying such a label reader a wise investment and the consumer can rest assured the handbag they purchase from this store is authentic.

CryptoMemory

CryptoMemory is EEPROM memory enwrapped within cryptographic logic. CryptoMemory offers hardware embedded cryptography with authentication technology that allows for Mutual Authentication and Secure Data Storage. The device offerings are highly flexible providing the versatility to incorporate into virtually any product.

Affordability

CryptoMemory is a low cost alternative to cryptographic microcontrollers. It offers an affordable alternative to secure microcontrollers without the financial cost or the complexity of integrating a microcontroller into a system. The purely logic-based cryptography in CryptoMemory eliminates the need for an operating system. Figure 1 depicts CryptoMemory's position within a Security-Price/Complexity chart of alternative products.

Figure 1. CryptoMemory's Security Offer

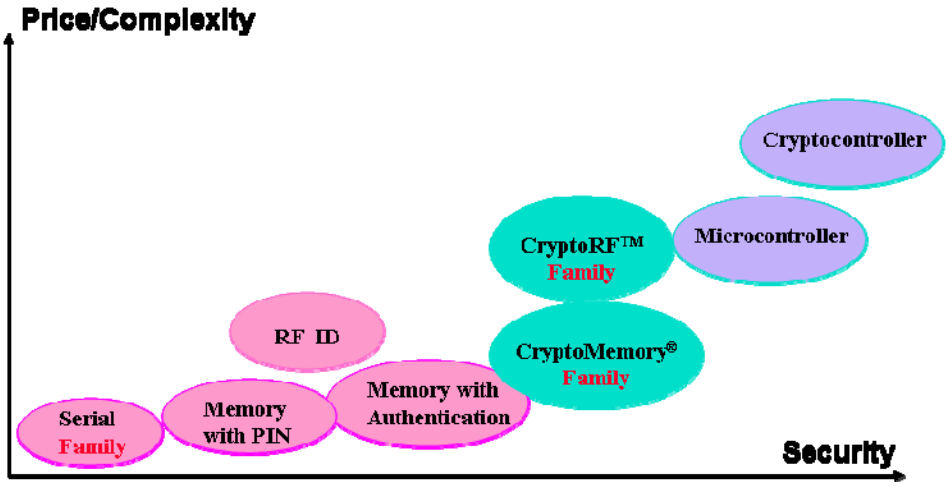
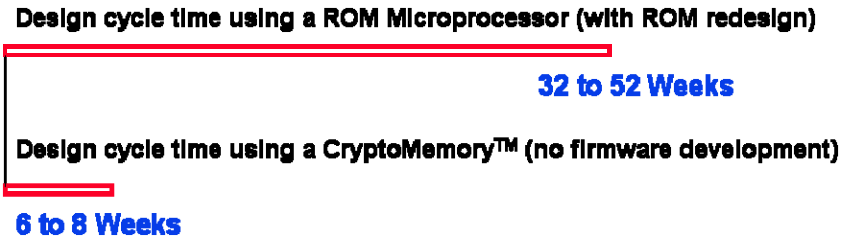


Figure 2 Illustrates the cost savings estimates of designing with CryptoMemory. CryptoMemory offers standard memory interfaces for easy integration into already existing systems. Alternative solutions involve operating system development which can require ROM masks for complete implementation. Against such a backdrop, CryptoMemory offers cost savings of 30% - 50%.

Figure 2. Time Savings designing with CryptoMemory



Competition

CryptoMemory has no competition. The mutual authentication technology, data encryption capabilities, and support for encrypted Message Authentication Codes (MACs) make it the only device of its kind in the market today. Closest in the form of competition are memories with some password protection ability from Infineon and Gemalto (formally Gemplus). Even the password solution offered is inferior to Atmel's solution which provides the additional option of using encrypted passwords. Table 2 summarizes the key differences between CryptoMemory and Competition. Notice the flexibility CryptoMemory offers in number of interfaces supported, device densities, user memory and memory zones on top of the already superior security.

Table 2. CryptoMemory versus Competition

Feature	ATMEL	Competitor Products		
	Atmel	Infineon	Gemplus	
Features	True Family of 9 Devices	SLE4442, SLE4428	GemClub Memo	GPM 2K, 8K
Protocol	2 wire, T=0, ISO 14443-B	I2C	T=0	I2C
Answer to Reset ISO 7816-3	yes	no	no	no
Interoperability with Microprocessor	yes	no	yes	no
Fast Transmission Baud Rate	yes	No	no	no
Total Memory	Up to 32K Byte	256 byte, 1K byte	256 byte	256 byte, 1Kbyte
Usable Memory	Up to 32K Byte	224 byte, n/a	224 byte	224 byte, n/a
Number of Zones	16	1	2	1
Selectable access rights per zone	yes	no	no	no
Password Security	yes	yes	yes	yes
Encrypted Passwords	yes	no	no	no
Dynamic Mutual Authentication	Yes, 64-bit key	no	no	no
Write Lock Mode	yes	no	no	no
Stream Encryption	yes	no	no	no
Read MAC	yes	no	no	no
Write MAC	yes	no	no	no
Operating Voltage	3V to 5V	5V	3V to 5V	5V

Typical Applications

The main applications of CryptoMemory are in the areas of product authentication and secure data storage.

Product authentication requires ability for secure identification. The authentication technology CryptoMemory offers makes it a suitable fit for virtually in any product that requires anti-counterfeit protection. These include consumables, pharmaceuticals, Intellectual Property, security passes, and piece-part authentication, and piece-part coupling (industrial hose connections, patient-drug compatibility checks etc.).

Data protection requires ability to protect the confidentiality and integrity of any piece of data of interest. CryptoMemory provides this ability through data encryption and use of encrypted MACs. Typical applications include secure storage of network keys, bulk data digests, identity cards, stored value (cafeteria, loyalty, transit, cards etc.), energy meters, and transaction records.

Device Description

CryptoMemory is an EEPROM memory with a 64-bit embedded hardware cryptographic interface. The memory is divided into separate configuration and user sections. The user customizes the security features and options of CryptoMemory by programming the configuration. CryptoMemory provides fuse bits that permanently lock the user security preferences in the memory. CryptoMemory comes in contacted interface as CryptoMemory and in a contactless interface as CryptoRF®.

Security Features

CryptoMemory offers 4 levels of security:

1. Free access for use as straight memory
2. Password protection using a choice of 8 sets of separate read/write passwords
3. Mutual Authentication using choice of 4 sets of 64-bit keys
4. Full Data Encryption for data confidentiality.

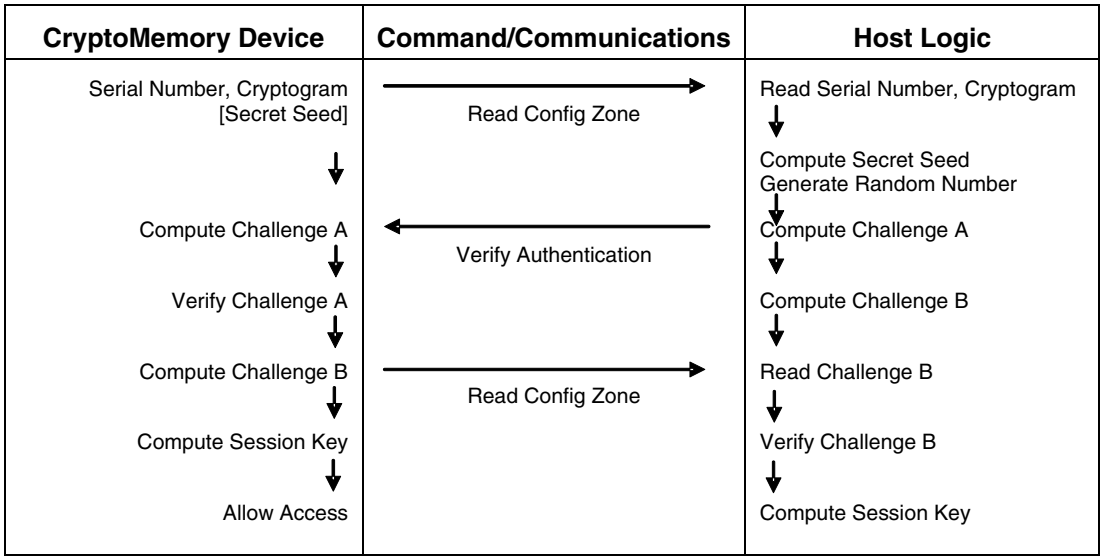
In addition, CryptoMemory offers encrypted Message Authentication Codes (MACs) for read and write operations used to verify the authenticity of the message source and integrity of message content. Understanding the protection CryptoMemory offers to combat counterfeiting requires some insight into the mutual authentication process.

The Mutual Authentication Process

CryptoMemory offers a random number enhanced mutual authentication protocol through which a host and the CryptoMemory device authenticate one another before any secure transactions. The mutual authentication protocol is based on a challenge-response scheme whereby each party verifies that the other has knowledge of some secret information that party possesses and does so without actual transferring the secret over the communication channel. The protocol starts with the host reading a cryptogram and identification information from the device. The host combines this information with additional information it possesses and a random number to generate a challenge for the device. It then sends this challenge together with the random number to the device. The CryptoMemory device utilizes the received random number and attempts to calculate the same challenge itself. If the challenge matches that received from the host, then the device updates its cryptogram and declares the host authentic. This is because the challenge is based on secret, non-readable information resident within the device which only an authentic host possesses knowledge of. To authenticate the device, the host calculates a new cryptogram, reads the newly calculated cryptogram from the device and compares the two. If they match, then the device is authentic. Only a device possessing

the secret the host expects it to have can generate a correct cryptogram. Figure 3 summarizes the mutual authentication process. Notice at no point does host or device secrets ever get transmitted over the communication channel thus making for powerful security.

Figure 3. CryptoMemory Mutual Authentication



Anti-Counterfeit Capability

CryptoMemory offers powerful anti-counterfeit protection to any product that embeds the device. When CryptoMemory stores product labeling information, the mutual authentication process guarantees only an authentic host can access that information. Counterfeiters would fall in the category of non-authentic hosts and so would not possess the ability to access information they need to duplicate in order to clone the product. This feature is powerful enough for anti-counterfeiting but CryptoMemory offers additional features to enhance this strength.

Ability to Personalize the Device

CryptoMemory allows for customization of security preferences and identification information, and offers ability to permanently lock this information within the device. Security preferences include choice of security level, secrets, passwords, and user defined contents of secrets and passwords. Identification information includes user definable device identification (serial) number, initial cryptograms, as well as additional fields provided for any additional custom identification. CryptoMemory offers 2 Kbits of configuration memory in addition to quoted device density. When configuration is complete, CryptoMemory provides fuses to blow in order to permanently lock the personalized configuration. Three separate fuses are available for this purpose to accommodate various manufacturing processes that require intermediate information locking.

Secure Storage of Secrets

CryptoMemory stores secrets in the configuration memory which are used in the mutual authentication process. To maintain high security, the device must never divulge these secrets. These secrets include 4 sets of 64-bit secret seeds, and 4 sets of 64-bits session encryption keys. CryptoMemory permanently lock these values after device personalization and guarantee these values can never be read. Hosts require knowledge of these secrets to generate the right challenge and only authentic hosts have this knowledge.

Key Diversification

The authentication protocol CryptoMemory utilizes allows for diversification of various secrets, cryptograms and identification information during device personalization. Diversification increases the strength of anti-counterfeit protection by ensuring no two pieces of the same product contain similar labels. Should any one item be compromised to provide a counterfeiter its label information, the damage done will be limited to just this one item.

Key diversification is done by the host during device personalization at a secure location. The process starts with programming unique identification information like serial and other numbers into the device. The device provides several fields for this purpose. While using some strong cryptographic algorithm, the host combines identification information from each device with other information external to the device including secrets known only to the host (host keys) to generate secret unique signatures for each device. Examples of such algorithms are hash functions like SHA and AES-CCM. The host then stores these unique and diversified secrets into the device as initial cryptograms, secret seeds, or session encryption keys. Blowing personalization fuses at the end of the personalization process permanently lock the secret seeds and session encryption keys inside the device from read or modify access.

Note that although CryptoMemory utilizes symmetric-key cryptography, the host and the device do not share keys. The host only requires knowledge of how to generate the key within the device based on its own secret key.

Dynamic Operation of Cryptographic Engine

The cryptography within CryptoMemory is dynamic in the sense that internal non-volatile registers update with successful cryptographic operations. This implies no two functionally equivalent operations are identical. For instance, in encryption mode, the encrypted text for any given clear text will always be different for all subsequent operations with the same device. This dynamism extends to Message Authentication Codes (MACs), session encryption keys and cryptograms. With such dynamism, the current state of the cryptographic engine at any time maintains ties to the initial values of initially programmed secrets and cryptographic transactional history. Such dynamism further strengthens the diversity of the devices thus enhancing resistance to counterfeit.

Random Number Enhanced Challenges

CryptoMemory utilizes 64-bit challenges during the mutual authentication process. Generation of these challenges involve the use of 64-bit random numbers to improve the strength of the challenge. The host generates the random number and has the freedom of adopting a random number generation of desirable quality.

Additional Data Protection Features

Use of data encryption and message authentication codes allows CryptoMemory to assure the confidentiality and integrity of any data requiring secure storage. In addition, CryptoMemory offers additional data storage features:

Modify Forbidden: Renders data under protection read-only.

Program Only: Constraints data modification to only comprise bit changes from logic "1" to logic "0" and not vice versa.

Write Lock: Allows flexibility to fine tune the granularity of the Modify Forbidden feature by rendering individual bytes within a zone read-only.

Anti-Tearing: Provides non-volatile buffering for data write operations. This protects against partial writes that may happen if someone prematurely pulls out a payment card from a vending machine (e.g. pay phone, food, etc.)

Program Only Mode: Allows flexibility to define multiple levels of access to a common resource. This works well in a multiple privilege access regime. CryptoMemory allows for assignment of different access requirements where supervisor privilege may have complete read/write access rights and normal privilege may only have read/program-only privileges.

Device Flexibility

CryptoMemory offers flexible features and options that allow integration into virtually any product. This section outlines some of the features:

Multiple Interface Support

CryptoMemory supports the following three communication interfaces:

Two-Wire Interface (TWI) for wired synchronous communications. This allows CryptoMemory to easily connect to any embedded microcontroller like ARM and AVR.

ISO 7816-3 interface in T=0 Mode for wired asynchronous communications. This allows CryptoMemory to communicate with any off-the-shelf readers that support this industry standard.

ISO 14443-B RF Interface for wireless communications. This allows CryptoMemory to communicate with any off-the-shelf readers that support this industry standard.

A True Family of Devices

CryptoMemory is a true family offering 9 densities from 1Kbit to 256Kbits. This provides the flexibility of choosing the right size so one does not overpay for memory. Table 3 lists the various densities offered.

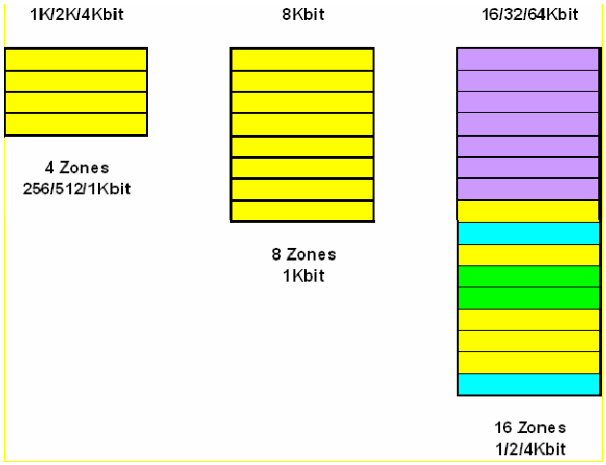
Table 3. CryptoMemory Device Densities

Memory Density	CryptoRF	CryptoMemory
1Kbit	AT88SC0104CRF	AT88SC0104C
2Kbit	AT88SC0204CRF	AT88SC0204C
4Kbit	AT88SC0404CRF	AT88SC0404C
8Kbit	AT88SC0808CRF	AT88SC0808C
16Kbit	AT88SC1616CRF	AT88SC1616C
32Kbit	AT88SC3216CRF	AT88SC3216C
64Kbit	AT88SC6416CRF	AT88SC6416C
128Kbit		AT88SC12816C
256Kbit		AT88SC25616C

Multiple Zones for Multi-Application Support

The user memory in each CryptoMemory device is divided into 4, 8, or 16 zones to allow support for multiple applications. The security requirements for each zone are independently definable with independent choice of various keys and passwords offered by the device. With such flexibility, it is possible to have multiple applications in the same device with security requirements ranging from free access to full authentication with data encryption. Assigning the same security requirements to all zones allow the zones to be effectively used as one large zone. Figure 4 illustrates the number of zones available within various CryptoMemory device densities and also the fact that single applications that pan multiple zones do not need to reside in contiguous zones.

Figure 4. CryptoMemory Zones



Common Feature Set

All CryptoMemory devices share the same security features and package options. All the security features and options are user customizable during personalization. A common platform of security features provides the flexibility of changing device densities with evolving needs without the penalty of redefining or reprogramming for the desired security.

Choice of Security Levels and Options

CryptoMemory provides the flexibility of choosing desired security level during device personalization. The choice of security levels includes free access, password protection, mutual authentication, full data encryption and combinations of any. This choice also includes choice of cryptographic keys and passwords that are independently assignable to zones. Furthermore, CryptoMemory offers additional security options to include Write Lock, Program Only, Anti-Tearing, and One Time Programmable features. The trade-off in choosing higher security levels is code space and timing requirements on the host side.

Pin Compatibility with Atmel Serial EEPROM

CryptoMemory offers full pin compatibility with Atmel's AT24Cxxxx family of serial EEPROM products. This allows the flexibility of security upgrade without the penalty of system redesign.

Example

Figure 5 depicts a driver license application example illustrating the perks of having multiple device densities and zones.

Figure 5. CryptoMemory Density Application Fit

Application Features	Kbit	Contact Device	RF Device
Basic ID Card	2K	AT88SC0204C	AT88SC0204CRF

ID Card + Finger Print	4K	AT88SC0404C	AT88SC0404CRF
ID Card + Finger Print + Picture	8K	AT88SC0808C	AT88SC0808CRF
ID Card + Finger Print + Picture + Driving Violations	16K	AT88SC1616C	AT88SC1616CRF
ID Card + Finger Print + Picture + Driving Violations + Health Data	64K	AT88SC6416C	AT88SC6416CRF

A country with many states and different requirements may implement the same basic data and security features for all cards. States requiring additional features may select larger memory sizes and control access with unique key sets if desired.

Physical Protection

CryptoMemory provides protection from physical attacks. It contains built-in tamper monitors to prevent operation in physically harsh environments. These include protection against illegal voltage, frequency, and temperature ranges. In addition, CryptoMemory obfuscates the configuration information in Memory to strengthen against physical attacks. CryptoMemory leverages on proven technologies from Atmel and on Atmel's security expertise in manufacturing security products.

Packaging

CryptoMemory is available in many flexible packaging options. It is deliverable in:

- Common 8-lead SOIC or PDIP plastic packages.
- Modules for smartcard applications.
- Tags for RFID or other wireless applications.
- Thinned wafers for embedding anywhere.

CryptoMemory is freely available for samples from Atmel Sales offices and samples in SOIC and PDIP plastic packages, as well as in contacted and wireless packages in smartcard form factors.

Help and Documentation

Development kits are available for various platforms for CryptoMemory. Development entails host side implementations that require detailed knowledge of the cryptography within CryptoMemory.

Documentation is also available. Most of the documentation is freely available on Atmel's website while more documentation describing the cryptography is available under Non-Disclosure and Limited Licensing Agreements (NDA and LLA) from Atmel.

More Help Coming in May 15, 2007

Current CryptoMemory kits require host side implementations that are time consuming. Coming in May 15 is the release of AT88SC-DK1, a development kit Atmel is releasing to alleviate the development effort needed to deploy CryptoMemory. This kit contains development libraries that capture host side implementations and present the user with a low-function count API. The libraries were development in C and compiled using GNU tools for versatility.

Editor's Notes About Atmel Corporation

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 www.cryptomemory.com.

Contact: Eustace Asanghanwa, Crypto & RF Memory Applications, Colorado Springs, Colorado, USA, Tel: (719) 540-6689, e-mail: easanghanwa@cso.atmel.com

Mouser Electronics

Authorized Distributor

Click to View Pricing, Inventory, Delivery & Lifecycle Information:

Atmel:
AT88SC-DK1