Programming the CryptoMemory® Device for Embedded Applications

CryptoMemory provides a cost-effective solution for securing sensitive data in non-volatile memory within any system. Various security features are built into CryptoMemory, and the user has the option of defining which features will be used for different data elements that may be stored.

To prepare CryptoMemory for use, several registers are programmed to indicate the selected security features to be used, and the appropriate passwords and keys are loaded into the device. Very little programming is needed to initialize the device. Depending on the options selected, only a few bytes up to a maximum of 2 Kbits of the configuration zone need to be programmed.

This application note describes the process of organizing data and determining security settings and the proper sequence for writing to CryptoMemory. This initial programming, or initialization, is typically done before the device is mounted to the board in the final application. The design of the application will determine what data is written during this initialization of the CryptoMemory device.

CryptoMemory®

Application Note

5051A–SMEM–01/04

Default Device Configuration

CryptoMemory devices are fully tested at Atmel. All functions are verified, and all memory locations are tested and then set to default values. These values are:

- User Zones – All user zones (4, 8, or 16) are programmed to all ones ($FF) throughout the entire zone.
- Configuration Zone: Answer to Reset – This field of the configuration zone is programmed to a preset value. The value programmed includes two bytes that indicate the memory density.
- Configuration Zone: Fab Code – This field is programmed to a preset value.
- Configuration Zone: Lot History Code – This field is programmed to a preset value. This field is locked and cannot be changed after leaving Atmel.
- Configuration Zone: Secure Code – This field, also known as the Write 7 Password, is programmed to a preset value.
- Remaining Configuration Zone – All remaining fields in the configuration zone are programmed to all ones ($FF). This includes all access and password key registers, all encryption keys, and all passwords except the secure code. In this configuration, access to all user zones is open and free.

Determine Initial Data and Security Settings

The first step in initializing CryptoMemory is to determine what data will be stored in the device and the structure for that data. Data may be thought of as different files, and these files will need to be organized within the various user zones of CryptoMemory. The security requirements for each file should be determined. Files with identical security requirements may be placed in the same user zone. If a file or group of files requires more than one user zone, multiple user zones may be set with the same security requirements to accommodate the large data files. In most cases, the design of the application will determine the data structure and security settings for CryptoMemory.

Initial Data

With the data structure established, determine what data should be written to the device during the initial programming. This is typically data that needs to be in the device before it is installed on the board. In addition to the user zones, there is also a 4-byte card manufacturer code and a 16-byte issuer code that may be programmed in the configuration zone as part of initialization.

Security Settings

The next step is to determine the security requirements of the application and how each zone of the CryptoMemory needs to be protected. Each user zone has one access register and one password key register, allowing the security requirements for each zone to be set independently. If multiple zones are required to store large data files, they may be set to the same security requirements. CryptoMemory offers a variety of security options; these options can be explored using the CryptoMemory Evaluation Kit (AT88SC25616C-EK). Security options are also documented in the CryptoMemory Embedded Specification, available under NDA. Briefly, the available security options are:

- Open or free access: no restrictions for read or write of a user zone.
- One-time programmable: the data programmed during initialization is locked and may not be changed.
- Program only: the data programmed during initialization may only be changed from a logic value "1" to logic "0" on a bit-by-bit basis. This can be used for a countdown function.
- Write protect: the data programmed during initialization may be protected byte by byte within a user zone.

- Password protection: separate passwords may be required for read and/or write privileges to the user zone; eight separate password sets are available.
- Authentication protection: a successful authentication sequence is required for read and/or write privileges to the user zone; four separate key sets are available.
- Encryption required: after a successful authentication, data is required to be encrypted for both read and write operations to the user zone.

The above list is not exhaustive, and various combinations of these security options may be implemented.

Writing to CryptoMemory

Once the data structure, initial data, and security settings have been established, this information must be written into the CryptoMemory device. This is accomplished by following the sequence below. Once the data is written and the security fuses are set, the device is ready for use in the end application. Details of the commands used and a simple example are included in this document.

Write Data to User Zones

In the default configuration from Atmel, all user zones have free access rights. Writing initial data into the user zones should be done before setting security configurations. Use the *Set User Zone* command and *Write User Zone* command to write initial data into the user zones. The *Read User Zone* command may be used to verify the data written.

Unlock Configuration Zone

Before any data can be written to the configuration zone, it must be unlocked by presenting the correct security code (Write 7 Password). Use the *Verify Secure Code* command with the proper password supplied by Atmel to unlock the configuration zone. Use the *Read Configuration Zone* command to read back the security code at address $E9 for verification that the configuration zone has been unlocked.

Write Data to Configuration Zone

Data contained in the configuration zone is divided into four types of information:

CODES: These include the answer to reset value, fabrication zone, identification number, card manufacturer zone, and issuer zone. The information programmed in these areas may be used by the application as determined by the application developer. The answer to reset and fabrication zone codes are programmed to default values by Atmel but may be modified. These codes are all write protected once all security fuses have been set.

REGISTERS: For each user zone, there is one 8-bit access register and one 8-bit password/key register. These registers are used to define the security requirements for each user zone. In addition, there is one device configuration register that determines several options affecting the security of all user zones globally.

KEYS: There are four sets of keys (Secret Seeds) used for authentication and four sets of keys (Session Keys) used for encryption; each key is 64 bits long. There are also four initial cryptogram values that may be defined and one identification number used with all four sets of keys.

PASSWORDS: There are eight sets of passwords; each set consists of a read access password and a write access password.

Writing this data is accomplished by performing the *Write Configuration Zone* command at the appropriate location. The *Read Configuration Zone* command may be used to verify the data written. Please consult the CryptoMemory Embedded Specification for proper memory address within the configuration zone for each data field. As soon as

values are written to the registers, keys, and passwords, they become effective in determining the security of the user zones.

Set Security Fuses

Three security fuses protect the information contained in the configuration zone.

FAB FUSE: This fuse protects the answer to reset value and the fabrication zone. These areas are write-protected and cannot be changed once the fab fuse is set.

CMA FUSE: This fuse protects the card manufacturer zone. This area is write-protected and cannot be changed once the CMA fuse is set.

PER FUSE: This fuse protects the rest of the configuration zone. The issuer code is write-protected and cannot be changed once the PER fuse is set. All registers, keys, and passwords are write-protected once the PER fuse is set. Modifications to these areas are only permitted by the internal logic; further detail may be found in the CryptoMemory Embedded Specification. One exception is the eight password sets. Once a write password is properly presented, only the read and write password in that set can be modified by using the *Write Configuration Zone* command. Once the PER fuse is set, the secure code (Write 7 Password) will no longer give access to the configuration zone.

These three fuses must be set in the order listed above (FAB, then CMA, then PER). The *Write Fuse* command is used to set each of the three fuses individually. The Address 2 value for setting each fuse is shown in Table 1 below.

Table 1. Write Fuse – Fuse ID

Fuse	Address 2
FAB	$06
CMA	$04
PER	$00

The *Read Fuse Byte* command may be used at any time to check the status of all three fuses.

Table 2. Read Fuse Byte – Returned Data

Fuse Condition	Fuse Byte	
No Fuses Set	XXXX	0111
FAB Set	XXXX	0110
FAB, CMA Set	XXXX	0100
FAB, CMA, PER Set	XXXX	0000

Synchronous Communications

CryptoMemory communicates by using a synchronous two-wire serial protocol. This two-wire serial interface is identical to that used on Atmel's AT24Cxxx family of serial EEPROMs but with a larger unique command set to support the various security functions. Synchronous communications may be performed with a clock speed of up to 1.5 MHz.

Command Set

There are a total of 16 commands for communicating with CryptoMemory. Only eight commands are required for the initial programming. The command set used for initializing CryptoMemory is shown in Table 3.

Table 3. Initialization Command Set

		Command	Addr 1	Addr2	N	Data (N)
Write User Zone		$B0	addr	addr	N (1)	N bytes
Read User Zone		$B2	addr	addr	N	
System Write	Write Config Zone	$B4	$00	addr	N (1)	N bytes
	Write Fuses		$01	fuse ID	$00	
	Set User Zone		$03	zone	$00	
System Read	Read Config Zone	$B6	$00	addr	N	
	Read Fuse Byte		$01	$00	$01	
Verify Secure Code		$BA	$07	$00	$03	3-byte password

Note: For AT88SC0104C–AT88SC1616C, N < $10
For AT88SC3216–AT88SC25616C, N < $80

Command Format

Each command sent to CryptoMemory must have 4 bytes: Command, Address 1, Address 2, and Parameter N. The last byte, N, defines the number of any additional data bytes to be sent to or received from the CryptoMemory device. Each command ends with a stop condition, for proper operation acknowledge polling must be performed after each command until the CryptoMemory device indicates it is ready for the next command. The formats for the three types of commands used for the initial programming are shown in Figures 1–3.

Figure 1. Write Command with N = 0 *(Write Fuses, Set User Zone)*

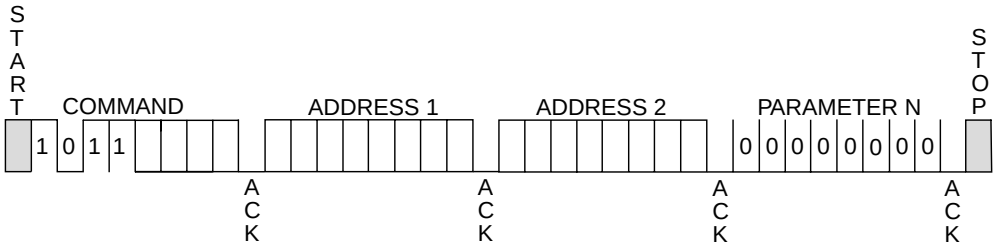


Figure 2. Write Command with N Bytes *(Write User Zone, Write Config Zone, Verify Secure Code)*

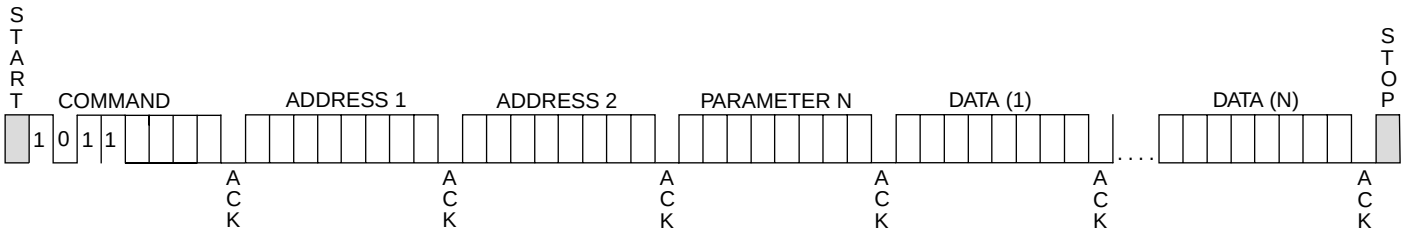
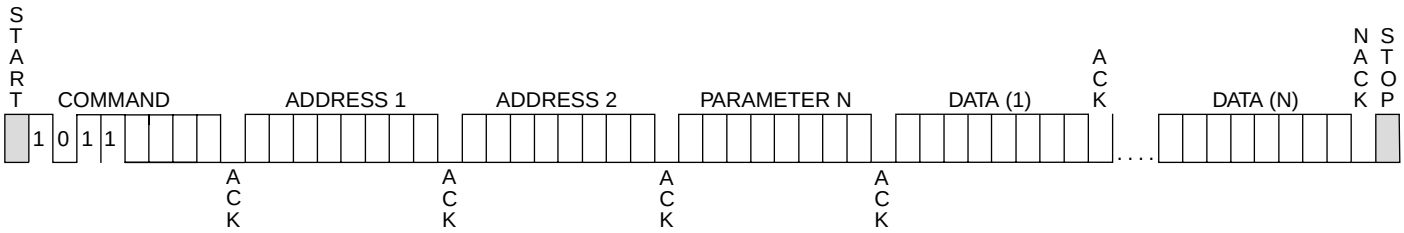


Figure 3. Read Command with N Bytes *(Read User Zone, Read Config Zone, Read Fuse Byte)*



Initialization Example

The AT88SC0104C is used for this example. A small pattern is written into each of the four user zones. Security for each of the four user zones and the associated register values are shown in Table 4. Simple values for codes, keys, and passwords are used.

Table 4. Security Settings (AT88SC0104C Example)

User Zone	Data	Security Requirements	Access Register	Password/ Key Register
0	Zone 0 Data	None	$FF	$FF
1	Zone 1 Data	Read/Write Password (Set 1)	$7F	$F9
2	Zone 2 Data	Read/Write Authentication (Set 2)	$DF	$BF
3	Zone 3 Data	Read/Write Password (Set1), Read/Write Authentication (Set 2) with Encryption Required	$57	$B9

The following example shows the two-wire commands sent to the CryptoMemory device for the purpose of initializing the device for use on a board. The flow is consistent with the steps described in this application note, and comments have been added as indicated with an asterisk (*).

```
*AT88SC0104C Initialization Example

*WRITE DATA TO USER ZONES
*Set User Zone 0
B4 03 00 00

*Write data = Zone 0 Data
B0 00 00 0B 5A 6F 6E 65 20 30 20 44 61 74 61

*Set User Zone 1
B4 03 01 00

*Write data = Zone 1 Data
B0 00 00 0B 5A 6F 6E 65 20 31 20 44 61 74 61

*Set User Zone 2
B4 03 02 00

*Write data = Zone 2 Data
B0 00 00 0B 5A 6F 6E 65 20 32 20 44 61 74 61

*Set User Zone 3
```

```
B4 03 03 00

*Write data = Zone 3 Data
B0 00 00 0B 5A 6F 6E 65 20 33 20 44 61 74 61

*UNLOCK CONFIGURATION ZONE
BA 07 00 03 FF FF FF

*WRITE CODES IN CONFIGURATION ZONE
*Write Card Mfg Code = P001
B4 00 0B 04 50 30 30 31

*Write Identification Number = 00000000012345
B4 00 19 07 00 00 00 00 01 23 45

*Write Issuer Code = STATION 035
B4 00 40 10 53 54 41 54 49 4F 4E 20 30 33 35 00 00 00 00 00

*WRITE REGISTERS IN CONFIGURATION ZONE
*Write Registers AR1/PR1 = 7F F9, AR2/PR2 = DF BF, AR3/PR3 = 57 B9
B4 00 22 06 7F F9 DF BF 57 B9

*WRITE KEYS IN CONFIGURATION ZONE
*Write Ci for set 2 = 22222222222222
B4 00 71 07 22 22 22 22 22 22 22

*Write Gc for set 2 = 5B4F9AE4B5098BE7
B4 00 A0 08 5B 4F 9A E4 B5 09 8B E7

*WRITE PASSWORDS IN CONFIGURATION ZONE
*Write Passwords, read 7 = 10 00 01, write 7 = 11 00 11
B4 00 B9 07 11 00 11 FF 10 00 01

*READ ENTIRE CONFIGURATION ZONE TO VERIFY
B6 00 00 F0

*Device Response:
3B B2 11 00 10 80 00 01 10 10 FF 50 30 30 31 FF
8C AD A8 10 0A AB FF FF FB 00 00 00 00 01 23 45
FF FF 7F F9 DF BF 57 B9 FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
53 54 41 54 49 4F 4E 20 30 33 35 00 00 00 00 00
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF 22 22 22 22 22 22 22 FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
5B 4F 9A E4 B5 09 8B E7 D8 FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF 11 00 11 FF 10 00 01
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

```
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

*SET SECURITY FUSES
*Set FAB Fuse
B4 01 06 00

*Set CMA Fuse
B4 01 04 00

*Set PER Fuse
B4 01 00 00

*Read Fuse Byte = X0
B6 01 00 01

*Device Response:
00
```

In-system Programming

The process described in this application note and the example given is intended for programming of the CryptoMemory device prior to mounting on the board. While this will simplify the operation of CryptoMemory in the end application, it is also possible to perform this initial programming in the final system. All the commands described here may be executed by the system into which CryptoMemory is incorporated. But to utilize the security features of CryptoMemory, this process of initialization must be performed before any information can be secured within the CryptoMemory device.

Atmel Corporation

2325 Orchard Parkway
San Jose, CA 95131
Tel: 1(408) 441-0311
Fax: 1(408) 487-2600

Regional Headquarters

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) 2721-9778
Fax: (852) 2722-1369

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

Memory
2325 Orchard Parkway
San Jose, CA 95131
Tel: 1(408) 441-0311
Fax: 1(408) 436-4314

Microcontrollers
2325 Orchard Parkway
San Jose, CA 95131
Tel: 1(408) 441-0311
Fax: 1(408) 436-4314

La Chantrerie
BP 70602
44306 Nantes Cedex 3, France
Tel: (33) 2-40-18-18-18
Fax: (33) 2-40-18-19-60

ASIC/ASSP/Smart Cards
Zone Industrielle
13106 Rousset Cedex, France
Tel: (33) 4-42-53-60-00
Fax: (33) 4-42-53-60-01

1150 East Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906
Tel: 1(719) 576-3300
Fax: 1(719) 540-1759

Scottish Enterprise Technology Park
Maxwell Building
East Kilbride G75 0QR, Scotland
Tel: (44) 1355-803-000
Fax: (44) 1355-242-743

RF/Automotive
Theresienstrasse 2
Postfach 3535
74025 Heilbronn, Germany
Tel: (49) 71-31-67-0
Fax: (49) 71-31-67-2340

1150 East Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906
Tel: 1(719) 576-3300
Fax: 1(719) 540-1759

Biometrics/Imaging/Hi-Rel MPU/
High Speed Converters/RF Datacom
Avenue de Rochepleine
BP 123
38521 Saint-Egreve Cedex, France
Tel: (33) 4-76-58-30-00
Fax: (33) 4-76-58-34-80

e-mail
literature@atmel.com

Web Site
http://www.atmel.com

5051A–SMEM–01/04