Protecting System Configuration Data with CryptoMemory®

NEARLY ALL EMBEDDED SYSTEMS USE SOME FORM OF NON-VOLATILE DATA STORAGE. CRYPTOMEMORY® NOW OFFERS A SECURE SOLUTION FOR STORING DATA IN A SYSTEM. THIS ARTICLE WILL DESCRIBE HOW TO USE CRYPTOMEMORY IN AN EMBEDDED SYSTEM TO STORE CONFIDENTIAL CONFIGURATION DATA.

By: Dale Anderson, Applications Engineer

In nearly all embedded systems today, some form of nonvolatile memory is used to store information required by the system for each use. This information could be settings from the last system use, preferences selected by the user, or configuration data programmed by the system manufacturer. In the case of configuration data, this often determines the performance features of the system and may be considered confidential by the system manufacturer. Take, for example, the consumer product offered at three different levels of performance and three different price points. For manufacturing efficiency, the electronics inside all three products are identical, and only the features that are enabled are different. The configuration data determines the features or levels of performance that will be enabled in the low-end, mid-range and high-end versions of the product. A knowledgeable consumer with an electronics background (and perhaps a little help from an Internet site) could purchase the low-end product and attempt to upgrade to the high-end version simply by reprogramming the system configuration data. Atmel's CryptoMemory device family offers a solution to protect this configuration data, the manufacturer's intellectual property and the manufacturer's profit margin.

	Memory Zone and Security Level		Access Register	Password Register
Zone 0 - Manufacturer's Configuration Data	$000		$D5	$3F
	-	64 bytes Encrypted		
	-	Read Protected by Authentification Key 0, No Write Allowed		
	$038			
Zone 1 - Manufacturer's Configuration Data	$000		$D5	$3F
	-	64 bytes Encrypted		
	-	Read Protected by Authentification Key 0, No Write Allowed		
	$038			
Zone 2 - User Data	$000		$D7	$7F
	-	64 bytes Encrypted		
	-	Read/Write Protected by Authentification Key 1		
	$038			
Zone 3 - Open Memory	$000		$FF	$FF
	-	64 bytes		
	-	Open Memory		
	$038			

Figure 1: Security Settings

CryptoMemory is a family of secure serial EEPROMs designed to protect the information they store. With memory densities from 1 Kbits to 256 Kbits, CryptoMemory is able to store and protect small to large amounts of data. User-defined memory partitioning provides both secure and open data storage in the same device. Access to secure memory portions is controlled by a mutual authentication protocol, encrypted passwords and data encryption. And with its 2-wire serial communications, CryptoMemory can be easily integrated into any embedded application.

Memory and Security Selections

The AT88SC0204C device has 2 Kbits of EEPROM memory arranged as four zones of 512 bits (64 bytes) each. The security access rights for each zone may be independently selected. To protect each zone, there are eight password sets and four authentication key sets available. For this example, we will elect to use the highest level of security, mutual authentication and stream encryption of data. We will use different keys to protect the manufacturer's configuration data and user's information. Additionally, we will lock the manufacturer's configuration data, so it cannot be rewritten even after proper authentication. Atmel's CryptoMemory Evaluation Kit (AT88SC25616C-EK) provides additional information on these and other CryptoMemory security options and provides a platform for experimenting with these options on real devices. Figure 1 shows the assignment of memory zones and security levels. Zone 0 and Zone 1 have the same security settings, providing 1024 bits (128 bytes) of memory for storage and protection of the manufacturer's configuration data.

These security selections are set by writing to access registers and password registers in a configuration zone of the device. This configuration zone is an additional 2 Kbits of EEPROM used to store security settings, passwords, authentication keys, and cryptograms, and this zone also provides an additional 61 bytes of one-time programmable (OTP) memory.

Programming CryptoMemory for Use

Once memory partitioning and security settings are determined, the AT88SC0204C may be programmed for use. Since the manufacturer's configuration data that we want to protect cannot be changed, it must

be written as the device is initially programmed. The device should be programmed in the following sequence. (The applications note, *Programming the CryptoMemory Device for Embedded Applications*, available on the Atmel website, provides more detailed information on this process.)

- Write user data. Any initial information that is to be stored in the device should be written into the four zones of the memory at this time. Since we will be preventing any future writes to Zones 0 and 1, the manufacturer's configuration data must be written at this time.
- Unlock the configuration zone. This is done by presenting the secure code (provided by Atmel) to the device.
- Write to the configuration zone. The access registers, password registers, initial cryptogram values and authentication keys to be used are all written to the configuration zone. Once these values are written, the security options selected take effect in protecting the user zones of CryptoMemory. If any information is to be stored in the OTP areas of the configuration zone, it should be written at this time.
- Write the security fuses. The last step in programming CryptoMemory is writing the security fuses to lock the configuration zone. This will hide the secret keys for authentication and prevent any further modifications to the configuration zone.

Programming CryptoMemory is accomplished by using the eight commands shown in Figure 2. Each command consists of four bytes where the last byte indicates how many additional bytes are included for a write command or how many bytes to expect back when reading the device. These commands operate to a simple 2-wire interface consisting of clock and data and may be implemented on commercially available memory programmers.

CryptoMemory in the System

After the AT88SC0204C is programmed, it is ready for installation in the system. The system may access Zone 3 by simply executing a Set User Zone command followed by the Read User Zone or Write User Zone command; there were no security conditions established for this zone so access is open. Access to User Zones 0, 1 or 2 will require a successful execution of the Verify Authentication command, using the proper key. Authentication involves a calculation and exchange of new 64-bit cryptograms by both the system logic and CryptoMemory device. Received values are compared against calculated values before access is granted to the protected user zone. These values will be different for each and every authentication between the system and CryptoMemory. After successful authentication, the Verify Encryption command is used to initiate data encryption. Only after this is accomplished can the protected manufacturer's configuration data in Zones 0 and 1 be read out in an encrypted form.

In addition to the logical protection of data stored in CryptoMemory, there are also tamper protection circuits on chip. Whether operating in a system or removed from the system and under attack in a lab, these circuits are designed to prevent any unauthorized access to the memory contents of CryptoMemory. All features combined provide a safe location for storing manufacturer's configuration data or any other sensitive information in a simple secure serial EEPROM. ■

		Command	Addr 1	Addr 2	N	Data (N)
Write User Zone		$B0	$00	addr	N ≤ $10	N bytes
Read User Zone		$B2	$00	addr	N	
System Write	Writi8ng Config. Zone	$B4	$00	addr	N ≤ $10	N bytes
	Write Fuses	$B4	$01	fuse ID	$00	
	Set User Zone	$B4	$03	zone	$00	
System Read	Read Config. Zone	$B6	$00	addr	N	
	Read Fuse Byte	$B6	$01	$00	$01	
Verify Secure Code		$BA	$07	$00	$03	3 byte password

Figure 2 : Commands for Programming