Card Cloning for Biochemistry Analyzers

Jaseela KA, Divya Unni

Department of Electronics, Vidya Academy of Science and Technology, Thrissur, Kerala, India

***Abstract*—A smart card, typically a type of chip card, is a plastic card that contains an embedded computer chip either a memory or microprocessor type that stores and transacts data. This data is usually associated with either value, information, or both and is stored and processed within the card's chip. The card data is transacted via a reader that is part of a computing system. Systems that are enhanced with smart cards are in use today throughout several key applications, including healthcare, banking, entertainment, and transportation.The objective of this project is to produce a cardcloning device for biochemistry analyzer using Verilog. Cardcloning involves the copying of card information at a card terminal using an electronic device or software, and then transferring the information from the master card into a number of slave cards. Biochemistry analyzer is a diagnostic equipment used to measure sugar, protein, cholesterol etc in the blood and urine sample for early detection and diagnosis of diseases. Such diagnostic equipments need a specific card for doing test. This card store testing parameters, details of reagents used and expiry date of the card. Password verification, authentication, data encryptions are used for securing data stored in this card. A specific card is needed for specific equipments. A single card is used for a few numbers of experiments. After this set of experiments we have to replace the card. So a large number of cards are needed for an equipment. By using this cloning device a large number of cards can be produced within a short time.**

***Index Terms*—Cardcloning.**

I. INTRODUCTION

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, midrange 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. Atmels CryptoMemory device family offers a solution to protect this configuration data, the manufacturers intellectual property and the manufacturers profit margin. CryptoMemory is a family of secure serial EEPROMs designed to protect the information they store.With memory densities from 1 Kbits to 256 Kbits, Crypto Memory 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.

.

Fig. 1. Proteinanalyzer with card

II. PROPOSED SYSTEM

Atmel cryptomemory AT88SC1616C through I2C communication. Atmel AT88SC1616C is a secure serial EEPROMs designed to protect the information they store. With memory densities from 1 Kbits to 256 Kbits. Crypto Memory is able to store and protect small to large amounts of data. Figure 2 shows Proposed Blockdiagram .It consists of PSOC3 controller, Interface device ,status LED. Interface device consists of many slots. Slots contain many cards. We are cloned same information on all cards by using I2C.Status LED is used for indicating information is written into card is successfully. If information is successfully written LED is glow. Otherwise not. Cardsense pins in used for indicating card are placed into correct position of the slot. Cardpower pins used for giving power into cards.

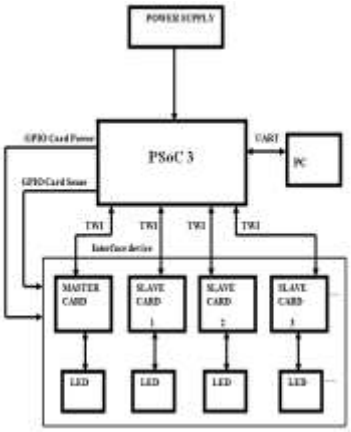

Fig. 2.Blockdiagram

III. HARDWARE COMPOSITION

A. Atmelcryptomemory AT88SC1616C

1) Memory and Security Selections

The AT88SC1616C device has 2 Kbits of EEPROM memory arranged as sixteen zones of 128 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 manufacturers configuration data and users information. Additionally, we will lock the manufacturers configuration data, so it cannot be rewritten even after proper authentication. Atmels 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 4 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 manufacturers configuration data.

Fig. 3. Atmelcryptomemory AT88SC1616C

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 onetime programmable (OTP) memory.

2) Programming CryptoMemory for Use

Once memory partitioning and security settings are determined, the AT88SC0204C may be programmed for use.

Since the manufacturers 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.

- Write user data. Any initial information that is to be stored in the device should be written into the four zones Fig. 3. Atmelcryptomemory AT88SC1616C Fig. 4. security settings of the memory at this time. Since we will be preventing any future writes to Zones 0 and 1, the manufacturers 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.

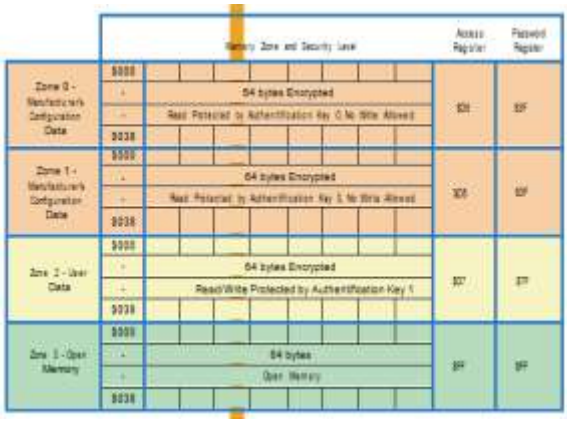

Fig. 4. security settings

Programming CryptoMemory is accomplished by using the eight commands shown in Figure 5. 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.

		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	Writißng 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	$0 0	$01	
Verify Secure Code		$BA	$07	$0 0	$03	3 byte password

Fig.5. Commands for Programming

3) Cryptomemory in the system.

After AT88SC1616C 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 Crypto Memory 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 manufacturers configuration data in Zones 0and 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 manufacturers configuration data or any other sensitive information in a simple secure serial EEPROM.

B. Microcontroller

PSoC is a true programmable embedded SoC integrating congurable analog and digital peripheral functions. It also contains a microcontroller and memory on a single chip. These chips contain a CPU core and several arrays of integrated analog and digital peripherals. A core, congurable analog and digital blocks, and programmable interconnect are included in a PSoC integrated circuit. The biggest difference of PSoC from other microcontrollers is the congurable blocks. PSoC3 is a redesign kit of development tool chain. The analog blocks can be redesigned to achieve better performance and handling. PSoC 3 has 8051 core. PSoC has three types of input output system as general purpose input output (GPIO), serial input output (SIO) and universal serial bus input output (USBIO). Here any GPIO can be connected to any peripheral routing. Any bus or path is wakeup on analog, digital or I2C match. In PSoC programmable slew rate reduces power and noise by using 8 different congurable drive modes. PSoC provide programmable input threshold capability for SIO also auto and custom/lock able routing is present in PSoC creator. 8051 specific SFR registers are present. The access port data registers through SFRs. External Data space (XDATA) is of 16 MB. Where up to 8 KB of SRAM on lead devices, all PSoC peripheral and configuration registers, EEPROM, ash memory and external memory interface (EMIF) are easily connect to PSoC kit. PSoC is similar to an ASIC: blocks has a wide range of functions and interconnected on chip. No special manufacturing process is required to create the custom configuration. PSoC is also similar to an FPGA.

In FPGA it must be configured at power up, but this configuration occurs by loading instructions from the built-in Flash memory. PSoC is most closely similar to a microcontroller combined with a PLD. To interact with the user-specified peripheral functions (called Components) code is executed, using automatically generated APIs. PSoC Creator generates the startup configuration code. Using congurable analog and digital blocks, designers can produce embedded applications. UDBs provides hardware capability to implement components from a rich library of pre built, documented and characterized components in PSoC creator. PSoC creator will create and connect components automatically. Here ne configuration granularity enables high utilization of silicon. Digital signal interconnect (DSI) routing allows any function in the UDBs to communicate with other on chip function or general purpose input output (GPIO) pin with 8 to 32 bit data buses. PSoC has three types of input output system as general purpose input output, serial input output and universal serial bus input output. Any GPIO can be connected to any peripheral routing. In PSoC slew rate reduces power and noise by different congurable drive modes.

PSoC provides programmable input threshold capability for SIO also auto and custom/lock able routing is present in PSoC creator. Analog blocks are of two types. Some chips of PSoC present with lots or less analog systems. Exact configuration depends on the product family. PSoC provide exible routing to all GPIO which are analog input/output, delta-sigma ADC up to 20-bit resolution. PSoC creator PSoC Creator is the second generation software IDE to design, debug and program the PSoC 3 / 4 / 5 devices. PSoC Creator also allows much freedom in assignment of peripherals to I/O pins.

IV. SOFTWARE REQUIREMENTS

PSoC Creator helps to configure and program analog- and digital-peripheral functionality by using a Cypress PSoC device. Using PSoC Creator, can select and place Components, write C and/or Assembly source, and debug and program the project/part. This dynamic hardware-software combination allows you to test the project in a hardware environment while viewing and debugging device activity in a software environment When it using with associated hardware. PSoC controller allows C programming and Verilog programming. Verilog HDL has parallel and sequential execution where C only handles sequential instructions. In PSoC digital subsystem support Verilog and analog subsystem support C program. Using the digital programmable system makes application specific combinations of both standard and advanced digital peripherals and custom logic functions of the digital subsystem. These peripherals and logic are then interconnected to each other . Any pin on the device, providing a high level of design flexibility and IP security. Features like capabilities and architecture of the digital programmable system are mentioned and there is no need to interact directly with hardware and register level the programmable digital system at the. PSoC Creator includes features like high level schematic capture graphical interface to automatically place and route resources similar to PLDs.

The analog programmable system provides application specific combinations of both standard and advanced analog signal processing blocks. These blocks are then interconnected to each other and as in the digital subsystem it also provide any pin on the device, with a high level of design flexibility and IP security. The features of the analog subsystem are mentioned here to provide an overview of capabilities and architecture.

V. SIMULATION RESULT

Figure 6, 7 shows simulation result of writing and reading of data into smartcard during cardcloning.

Fig. 6.Reading data from smartcard.

Fig. 7.Writing data to smartcard.

Fig. 8.Cloning device

VI. CONCLUSION

This paper presents how store testing parameter of biomedical diagnostic equipments into Atmel cryptomemory card very securely through I2C communication protocol also producing a card cloning device using verilog HDL.

ACKNOWLEDGMENT

We would like to show our gratitude towards Dr.Sudha Balagopalan, Principal, Vidya Academy of Science and Technology for giving us sole co-operation and encouragement. We thank Dr.S.Swapna Kumar, HOD for assistance and Sruthi.M, Co-ordinator for the comments that greatly improved the manuscript. We thank our colleagues who provide insight and expertise that greatly assisted the project work.

REFERENCES

[1] Radha RC,Ravuri Aneeshkumar, “Design and implementation of I2C protocol on FPGA for EEPROM”, International Journal of Scientific & Engineering Research, Volume 5,

[2] Flavio D,Garcia, Peter van Rossum, Verdult, Ronny Wichers Schreur, “Dismantling SecureMemory, CryptoMemory and CryptoRF”second international conference on information security and cryptography September 2015.

[3] Amin Abd Elwahab, Ayman M. WahbaA, Amin Abd Elwahab,`` SecurityLayer for Smart Card Applications Authentication” International conference on theory.

[4] Dale Anderson,``Protecting system configuration data with cryptomemory” ,international journal of scientific & engineering research ,july 2009.