論文2000-37SD-1-8

자체 테스트 및 보안기능을 갖는 공중전화 카드 IC 설계

(Design of Phone Card IC with Security and Self-test Features)

朴 台 根 *

(Tae-Geun Park)

요 약

본 논문에서는 자체 테스트기능과 보안기능을 갖춘 공중전화 카드 IC를 검증함으로써 향후 공중전화 시스템의 국산화에 응용 가능성을 확인한다. 본 연구에서 설계된 공중전화용 IC는 10개의 명령어를 지원하고 금액 등 여러 가지 정보를 저장할 수 있는 비휘발성 메모리를 갖는다. 하나의 직렬 I/O로써 이루어지는 외부와의 통신 때문에 야기되는 테스트 시간 문제를 보완하기 위해 대부분의 테스트가 칩 내부에서 동작하도록 자체 테스트 기능을 추가하였다. 또한 여러 가지 보안기능이 소프트웨어, 하드웨어적으로 구현되었다.

Abstract

This paper proposes a design of phone card IC with the self-test features and the hardware and software security functions. We design and verify the proposed functions with modeling the terminal system environment. The proposed phone card IC provides 10 instructions and a non-volatile memory block containing the manufacturer / issuer / user information, the unit (money) value, and the security key. The self-test functions are designed to improve the test time degradation due to a serial I/O communication. Also some security features are implemented using hardware and software approaches.

Ⅰ. 서 론

현재 보편적으로 쓰이는 공중전화용 카드는 마그네틱 카드로서 그 안에 기본적인 정보(금액, 상태정보, 등) 만을 갖기 때문에 제공되는 기능이 단순하고 외부의 자기장 등에 민감하여 오류 발생률이 많다. 또한 치명적인 단점은 내부 정보의 유출과 변조가 용이하고 오용 또는 도용이 쉬워 무단복제 시 큰 손실이 예상된다. 실제 한해 이로 인한 손실과 금액 삭제로 인해 들어오는 민원으로 부가비용이 상당히 크다고 한다.

* 正會員, 가톨릭大學校 컴퓨터 電子工學部

(Department of Computer & Electronic Engineering, The Catholic University of Korea)

接受日字:1999年5月31日, 수정완료일:1999年11月9日

최근 보안성이 요구되는 분야에 많이 응용되는 IC카드를 이용하면 카드 당 단가는 마그네틱 카드에 비하여 높지만 여러 가지를 감안할 때 경쟁력 있는 방법으로 이미 프랑스, 독일 등 유럽 여러 나라에서 실제 이용되고 있다. 최근 우리나라에서도 외국 제품을 구입하여 공급하고 있는데 그에 대한 대체 제품의 조속한 개발이 시급한 실정이다. 현재 보편적으로 사용되는 제품 중에는 Siemens사의 SLE4436[1]이 있는데 이 제품의 메모리 영역은 221bit의 EEPROM/PROM과 16bit의 Mask ROM으로 구성된다. 특징적인 보안기능으로 Anti-tearing 기능과 카운터를 지원한다. Anti-tearing 영역은 비정상적으로 카드를 단말기로부터 제거했을 때에 카운터의 금액정보를 보호하는 역할을 담당하고 카운터는 금액의 감산 시 오류가 나지 않도록 설계되었다.

공중전화 카드는 COB 형태로 패키지된 IC를 내장하고 그의 구조는 이미 ISO-7816[2]으로 표준화되어 있다. 그의 내부에는 기능블럭으로 EEPROM, 인증블럭, 보안회로, 간단한 제어기 등이 내장되어 단말기(공중전화기)와 하나의 데이터 라인으로 비동기(혹은 동기) 통신에 의해 정보를 주고 받는다. EEPROM은 제조자/발행자/사용자 정보, 전달코드(Transport Code: TC), 인증키(Authentication Key), 금액 등의 중요한 정보를 저장하고, 인증블럭은 카드의 진위를 확인하기 위한 인증기능을 수행하며 외부에서 입력되는 Challenge에 대하여 응답한다. 보안회로는 입력전압이 불안정하면 EEPROM의 프로그래밍의 신뢰도가 저하되므로 이 때 프로그래밍 기능을 금지시킨다. 이러한 응용분야의 IC는 EEPROM의 신뢰도, 즉 데이터 보존기간과 Program/Erase의 싸이클링 회수가 중요하다. 그리하여 본 연구에서는 EEPROM에 대한 성능테스트를 위해 여러 가지 테스트 패턴 즉, Erase All/Program All/Diagonal/Column Check /Checker Board 등을 삽입하였다. 인증 알고리즘에 관해서는 일반적으로 Smart Card IC와 같이 범용 제어기가 내장되어 있고 고급의 보안 응용분야에 사용되는 경우에 훨씬 복잡한 알고리즘이 사용된다. 예를 들어 DES, Triple-DES[3],[4] 등과 같은 개인키(Private-key) 알고리즘은 내장 제어기를 이용한 Firmware로 구현이 가능하지만, RSA, ElGamal, Rabin[3],[4]등과 같은 공중키(Public-key) 알고리즘은 계산량이 많기 때문에 별도의 부연산기[5]를 설계하는 것이 일반적인 방법이다. 본 연구에서는 응용분야와 설계방향을 고려할 때 내부에 고정된 제어기(Hardwired -control) 방식으로 구현된 비교적 간단한 인증 알고리즘을 사용하였는데 알고리즘 개발 시 그의 복잡도 및 신뢰도 검증이 필수적이다.

2장에서는 제안된 공중전화용 IC 하드웨어의 구조를 정의하였고, 3장에서 하드웨어 설계에 대한 방법을 논하였고 결론은 4장에 제시하였다.

Ⅱ. 공중전화용 IC의 구조

1. 칩의 기능블럭

본 연구에서 제안된 공중전화 카드 IC의 구조는 그림 1에 나타내었고 그의 내부 기능블럭을 살펴보면 다음과 같다. EEPROM은 제조자/발행자/사용자 정보, 전달코드(Transport Code: TC), 인증키, 금액 등의 정보를 저장한다. 내부적으로 OTP(One-Time Programmable) 기능을 갖는 영역이 있으며 이는 하드웨어 및 소프트웨어의 방법으로 제어된다. 어드레스 부분은 EEPROM의 각 번지를 지정하는데 각 모드별, 영역별로 읽고 쓰고 지우는 기능이 제한되도록 설계된다. 프로그래밍 블럭은 EEPROM을 통해서 쓰고 지우는 명령을 수행할 때 내부적으로 고전압(약 15V)을 생성하고 이를 메모리블럭에 공급한다. 인증블럭은 카드의 진위를 확인하기 위한 인증기능을 수행하며 외부에서 입력되는 챌린지에 대하여 응답한다. Internal Signal Control Unit은 내부 기능블럭을 제어하는 기능을 담당한다. 각 모드 수행 시 적절한 메모리 영역 사용을 제어하며, 외부에서 주어지는 간단한 명령어를 해석/수행한다. 내부에 타이머를 갖고 있어 내부에서 사용되는 다양한 속도의 클럭을 만들고 외부 단말기와 비동기 직렬 통신을 제어한다. 또한, 인증 작업을 수행하며 EEPROM의 쓰고 지울 때 시간을 제어하여 신뢰도를 높인다. External Control Unit은 외부와 연결된 인터페이스 블럭으로서 직접 핀으로 연결되어 있다. 마지막으로 Blocking Unit은 입력전압의 상태를 주시하여 전압이 불안정하면 EEPROM의 프로그래밍의 신뢰도가 저하되므로 프로그래밍 기능을 금지시킨다.

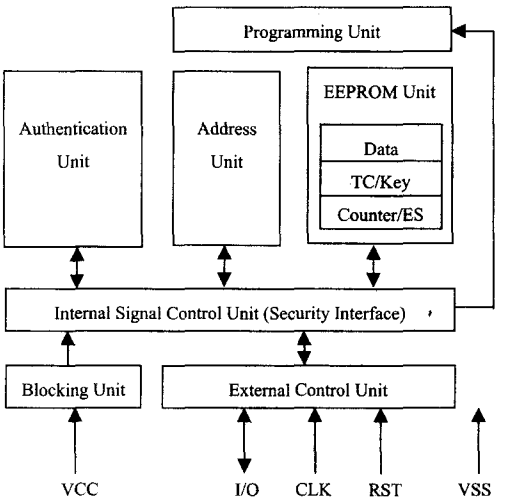


그림 1. 공중전화 카드 IC의 구조
Fig. 1. Structure of the phone card IC.

2. 메모리 구조 및 기능

공중전화 카드 IC에서 사용되는 내부 메모리는 표 1

에서 나타낸 것과 같이 총 1Kb(128바이트×8비트)의 EEPROM으로 구성되어 있고 각각 제조자 영역, 발행자 영역, 금액 E/S 영역, 금액 영역, 인증키 영역, 전달코드(Transport Code: TC) 및 에러 카운터 영역, 랜덤 넘버 영역, 그리고 사용자 영역으로 구분되어 있다.

제조자 영역은 칩 제조사, 제조년도, 주문자 코드, Lot Number 등과 같이 칩 제조와 관련된 정보를 제조 시 내부 패드를 이용하여 프로그램 하거나 기록한 뒤 Fuse 등을 이용하여 향후 변경하지 못 하도록 하고 읽기만 할 수 있다. 발행자 영역은 카드를 발행하는 기관(예: 한국통신)이 카드 발행과 관련된 정보를 기록하는 영역으로 읽기, 쓰기가 모두 가능하고, 발행자는 이 영역을 프로그램한 후 Lock의 명령어를 이용하여 이후 변경 불가능하도록 한다. 금액 E/S 영역은 에러에 의해서 금액 값이 바뀌었을 경우 금액의 백업용 보안 기능으로서 금액의 사용 실적을 표시하는 24 비트로 구성되어 있고 금액의 5%가 감액될 때 마다 하나의 비트를 프로그램하고 이 영역은 다시 지울 수 없어야 한다. 금액 영역은 실제 잔액을 표시하며 현재 금액보다 작은 금액을 쓰려고 할 때만 변경 가능하다. 전달코드 영역은 제조자로부터 발행자에게로 칩 전달 과정에서 분실/도난 등에 대한 보호를 위해 칩 제조 시 3 바이트의 전달코드를 기록하고, 발행자는 발행 시 올바른 전달코드를 제시해야 발행을 할 수 있다. 이 때 5번의 틀린 전달코드가 입력되면 카드는 스스로 Lock을 하여 자동 폐기된다. 전달코드가 일치할 경우 18-23 번지는 향후 인증키 영역으로 사용된다. 랜덤 넘버 영역은 카드 인증에 필요한 랜덤 넘버를 저장하는 영역으로 읽기/쓰기가 모두 가능하다. 마지막으로 사용자 영역은 부가 서비스를 위하여 다양한 사용자 데이터를 저장하는 영역으로 읽기/쓰기가 모두 가능한 영역이다.

동작 모드는 제조자, 발행자, 사용자 모드가 있으며 메모리의 각 영역은 각 모드별로 다르게 동작한다. 각 모드별 영역의 엑세스 허용상황은 표 2에 정리되어 있다. 제조자 모드에서는 칩을 제조한 뒤 제조자 영역과 전달코드에 필요한 정보를 기록한 뒤 나머지 영역은 지우고 카드의 정성동작을 확인한 후 발행자에게 전달한다. 발행자 모드에서는 올바른 전달코드를 제시한 뒤 발행자영역에 적당한 정보를 기록한다. 그리고 Lock 명령어를 이용하여 발행자 영역, 인증키 영역을 Lock한다. 카드의 정상동작을 확인하고 사용자에게 판매한다. 사용자 모드에서는 카드를 사용하면서 카드의 진위를

표 1. 공중전화 카드의 메모리 영역
Table 1. Memory map for phone card IC.

주소	내 용	영역	메모리 형태
0	칩 제조사 / 제조 년도	제조자 영역	OTP-ROM type by fuse or internal Pad
1	주문자 코드		
2	제조자 정보 예비		
3	Lot Number		
4	국가 코드	발행자 영역	OTP-ROM type by instruction lock
5	카드 종류 / 카드 권종		
6 9	발행자 정보 예비 영역		
10 12	카드 시리얼 넘버		
13 15	LSB 금액 E/S 영역 MSB	금액 E/S	Program-only EEPROM
16 17	금액 1(LSB) 금액 2(MSB)	금액 영역	EEPROM type
18 23	1.전달코드 (3 바이트) & Error Counter(1 바이트) 2.인증키	전달코드 정보 & 인증키 영역	OTP-ROM type by instruction lock
24 31	랜덤 넘버	사용자 영역	EEPROM type
32 127	사용자 정보 영역		

검사하는 인증 작업을 거치며 금액을 관리하고 사용자 영역을 이용하여 부가 서비스를 받을 수 있다.

표 2. 각 모드 대 영역별 access permission
Table 2. Access permission for Modes vs. Areas.

모드 / 영역	제조자 모드			발행자 모드						제조자 모드		
				TC Lock			TC Unlock					
	P	E	R	P	E	R	P	E	R	P	E	R
제조자	Y	Y	Y	N	N	Y	N	N	Y	N	N	Y
발행자	Y	Y	Y	N	N	N	Y	Y	Y	N	N	Y
금액 E/S	Y	Y	Y	N	N	N	Y	Y	Y	Y	Y	Y
금액	Y	Y	Y	N	N	N	Y	Y	Y	Y	Y	Y
TC	Y	Y	Y	N	N	N	Y	Y	Y	N	N	N
TC error	Y	Y	Y	N	N	Y	Y	Y	Y	N	N	N
인증키	Y	Y	Y	N	N	N	Y	Y	Y	N	N	N
Random	Y	Y	Y	N	N	N	Y	Y	Y	Y	Y	Y

3. 보안 기능

1) 발행자 확인을 위한 전달코드(Transport Code: TC)

칩 제조자에게서 카드 발행자에게로 카드가 전달되는 과정에서 발생될 수 있는 분실/도난 등에 대한 보호

기능으로서 전달코드를 알고 있는 발행자 이외에는 카드를 발급할 수 없게 하는 보안역할을 한다. 전달코드는 3 바이트로 구성되고 1 바이트의 TC 에러카운터 영역을 갖는다. 칩이 제조자에게서 카드 발행자에게 전달될 때는 EEPROM 영역 중 제조자 영역과 TC 에러카운터 영역만 읽을 수 있고 쓸 수 있는 부분은 에러카운터 영역 뿐이다. 카드 발행 시 올바른 전달코드를 칩에 입력하여야 TC Lock 상태에서 TC Unlock 상태로 바뀌면서 TC 및 TC 에러카운터 영역이 인증키 영역으로 바뀌고 발행자 영역, 금액 E/S 영역, 금액 영역, 인증키 영역, 랜덤 넘버 영역, 사용자 영역의 읽기/쓰기 기능이 가능하다.

카드 발행자가 카드를 발급하기 위해서는 외부에서 올바른 전달코드를 입력하여 확인하는 과정을 거치는데 임의의 코드를 무한정 시도하는 것을 막기 위하여 TC 에러카운터를 이용하여 5번으로 제한한다. 5번을 초과하여 오류가 발생하면 더 이상의 외부에 응답하지 않고 칩 스스로 폐기되는 기능을 갖는다.

2) 인증(Authentication)

카드의 진위를 판별할 수 있는 보안 메커니즘으로서 카드가 인증될 때에는 인증키와 금액정보 및 단말기에서 보내오는 랜덤 넘버를 사용하여 인증 알고리즘을 통하여 암호화된 데이터가 단말기로 보내져 카드의 사용허가가 나게 되므로 비밀 코드인 인증키는 높은 보안이 유지되어야 한다. 인증키는 사용자 모드에서는 그 코드의 변경이 불가능하며 외부로 유출이 금지된다. 인증키는 총 64 비트(인증키 : 48 비트, 금액 : 12 비트)로 구성되며 Challenge 데이터로서 랜덤 넘버는 64 비트로 구성되고 결과 데이터도 64 비트로 출력된다.

그림 2는 인증 과정의 구조도이다. 카드 발행 시 발행자가 인증키를 생성하여 칩 내에 저장한다. 단말기(전화기)에서 IC카드의 인증이 필요할 때에는 단말기 내부에서 64 비트의 랜덤 넘버를 생성하여 칩 내부의 랜덤넘버 영역에 기록한다. 그 후 단말기에서 IC카드로 인증을 명령하면 칩 내에 저장된 금액, 인증키와 전화기에서 보내온 랜덤 넘버를 이용하여 인증 알고리즘을 수행하여 그 결과(64 비트)를 단말기로 보낸다. 단말기는 IC카드에서 읽어 온 데이터와 내장된 마스터키를 사용하여 각 카드에 맞는 인증키를 생성하고 이 인증키와 금액, 랜덤 넘버를 이용하여 IC카드와 똑같은 알고리즘을 이용하여 계산된 결과를 비교한다. IC카드에서 읽어 온 결과와 자신이 생성한 결과가 같으면 계속 수행하고 만약 다르면 위조 카드로 인식하여 그에 따른 적절한 기능을 수행한다.

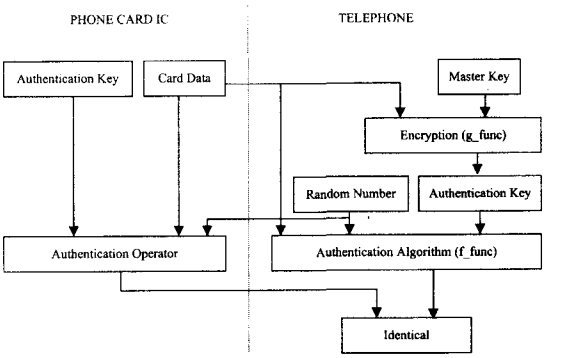


그림 2. 인증 블럭의 구조도
Fig. 2. Structure of the authentication block.

내부 메모리에 저장되는 여러 가지 데이터에 대한 신뢰도를 보장하기 위한 기능도 제공된다. 금액 데이터의 변경, 지워짐 등의 에러에 의하여 금액 값이 임의로 바뀌는 경우, 금액의 백업용 보안 기능으로서 금액의 사용 실적을 표시하는 24 비트로 구성되어 있다. 발행자가 카드 발행 단계에서 금액 영역에 처음 기록한 금액을 기준으로 금액이 5% 이상이 감액될 때마다 금액 E/S 비트를 프로그램 한다. 그리고 프로그램된 비트들은 다시 지울 수 없도록 설계되어 있다. 또한 칩에 공급되는 전압이 동작 중에 특정전압 이하로 내려갈 때 자동으로 리셋이 걸리며 칩이 초기화되며 그 때 진행되던 메모리 동작은 취소된다.

Ⅲ. 공중전화용 IC 설계

1. 하드웨어 설계 및 검증

본 연구에서 제안된 공중전화용 IC는 표 3에서와 같이 10개의 명령어를 지원한다. 각 명령어는 단말기에서 하나의 비동기 직렬 입력 핀을 통해서 칩으로 들어와 수행된다. 메모리 내용 변경을 위한 명령어는 수행의 간편함을 위해서 각 영역별로 세 가지로 구분하였다. 칩과 단말기는 주종관계로 동작하고 단말기에서는 송출한 명령어에 따라 일정한 시간 후에 응답을 기대하게 된다. 응답이 필요 없는 명령어일 경우에 단말기는 칩이 맞게 동작 했다고 가정하고 다음 작업을 진행한다. 표 3에는 IC Card에서 지원하는 10가지의 명령어를

나타내었다. 칩의 내부에는 테스트 및 사용 시 여러 모드를 선택할 수 있는 Speed/Mode 레지스터가 설계되어 있는데 각 비트별 기능은 표 4에 나타내었다.

표 3. 명령어 구조
Table 3. Instruction sets.

명령어	형 식	기 능
WRITE1	OPCODE+ADD1+ADD2+DATA	• 제조자/발행자/인증키 OPT 데이터 쓰기 • EEPROM 테스트
WRITE2	OPCODE+DATA1(LSB)+DATA2(MSB)	• 금액 영역 쓰기
WRITE3	OPCODE+ADD1+ADD2+DATA	• 사용자 영역 쓰기
LOCK	OPCODE	• LOCK cell 쓰기
READ	OPCODE+ADD1+ADD2	• EEPROM 데이터 읽기 • TC Error Counter 읽기
NOP	OPCODE	• No operation
TC	OPCODE+TC1+TC2+TC3	• 전달코드 비교
ES	OPCODE+ADD1+ADD2+DATA	• 금액 E/S 영역 쓰기
AUTH	OPCODE	• 인증
SPEED	OPCODE+DATA	• I/O 속도 변경

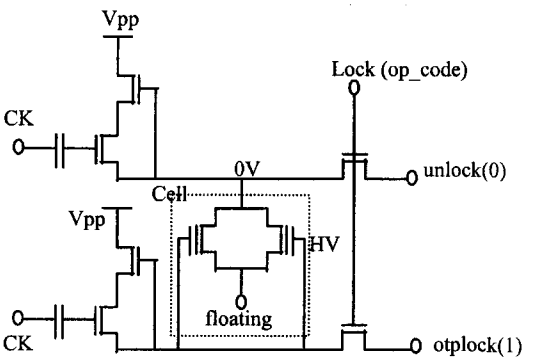
표 4. Speed/Mode 레지스터의 기능
Table 4. Functions of the Speed/Mode Register.

		형 식	기 능
[7:5]	001	EEPROM Test Mode	Erase All Pattern Test
	010		Program All Pattern Test
	011		Diagonal Pattern Test
	100		Column Check Pattern Test
	101		Checker Board Pattern Test
[4:3]	00	Normal Mode	Manufacturer Mode
	01		Issuer Mode (TC_LOCK=1)
	10		Issuer Mode (TC_LOCK=0)
	11		User Mode
[2:0]	000	I/O Speed Control	9.6 kbps
	001		19.2 kbps
	010		38.4 kbps
	011		153.6 kbps(Test Mode only)

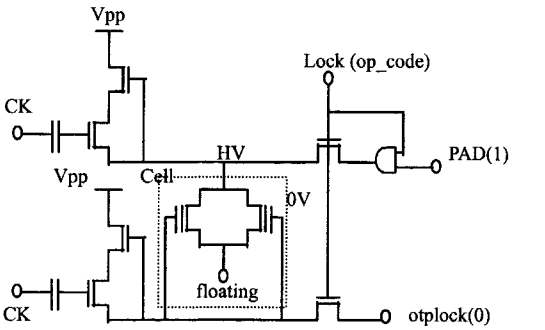
제안된 하드웨어는 Verilog 언어를 사용하여 모델링되었고 이를 검증하기 위하여 사용 시 서로 통신하게 되는 단말기 환경을 모델링하여 그의 모든 기능이 검증되었다. 이 때 사용된 테스트 기능은 다음 절에 자세히 나타내었다. 각 기능은 Verilog Simulator 상에서 검증되었고 신뢰도에 영향을 주는 EEPROM 블록은 그의 특성상 부득이 Behavioral-level에서 기술되어 검증되었다. 향후 표준셀 방식의 논리 회로와 EEPROM 블록을 이용한 ASIC 방법으로 실제 하드웨어를 설계해 검증하는 과제가 남아있다고 하겠다.

2. OTP Lock 셀의 구조

EEPROM 셀에 의한 OTP 영역의 쓰기/지우기 권한을 제조, 발급, 사용 시에 따라 각각 제한한다. 그림 3은 OTP Lock 셀의 구조와 Lock/Unlock 시의 동작상태를 나타낸다. 내부 승압회로에서 만들어진 Vpp(약 15V-17V정도)는 EEPROM 셀이 프로그램되거나 지워질 때 셀에 공급된다. 그림 3-a는 Lock상태를 나타내는데 EEPROM 셀의 게이트에 고전압(High-Voltage)이 인가되어 Floating gate에 전하가 존재하는 높은 문턱전압의 상태를 의미한다. 그림 3-b는 이와 반대로 드레인 쪽에 고전압이 인가되어 Floating gate의 전하를 빼내어 낮은 문턱전압 상태가 된다. 이 때 내부 PAD로부



a)Lock(EEPROM Erase) 상태



b) Unlock(EEPROM program) 상태

그림 3. OTP Lock 셀의 구조도
Fig. 3. Structure of OTP Lock Cell.

터의 신호가 Unlock 상태를 제어하게 되는데 이 단자는 웨이퍼 테스트 시에만 이용할 수 있고 패키지한 이후에는 사용할 수 없으므로 발급 후에는 Unlock이 불가능하다.

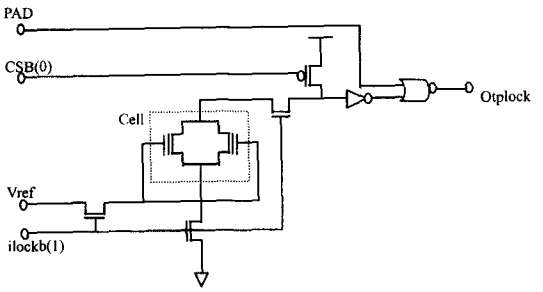


그림 4. OTP Lock 셀 읽기
Fig. 4. Reading of OTP Lock Cell.

그림 4는 Lock 셀의 상태를 읽는 방법을 나타낸다. 먼저 PAD의 입력이 1일 경우 즉, 칩 테스트 시에는 그림 3에서와 같이 1을 인가하여 값을 변경할 수 있고 제조 후에는 PAD 값이 0이 되어 그림 4의 출력을 허용해 준다. CSB 입력은 PMOS를 열어 셀에 전류가 흐르는지의 여부에 따라 출력의 값이 결정된다. Lock일 경우 지움(erase) 상태로 셀이 높은 문턱전압을 가지므로 출력은 1이고 Unlock일 경우 프로그램 상태로 셀이 낮은 문턱전압을 가지므로 출력은 0이다. 셀은 2개를 사용하였는데 시간에 따른 셀의 신뢰도를 고려한 것이다.

3. 테스트 기능

일반적으로 설계된 칩을 테스트하는 방법은 설계 시 사용한 테스트 패턴을 테스터의 규격에 맞게 바꾼 후 입력하여 출력을 옳은 해답과 비교하는 것이다. 그러나 본 공중전화 카드의 경우 입.출력 핀이 하나 밖에 없고 사용하는 프로토콜이 단순하고 느리기 때문에 위에 기술한 보편적인 테스트 방법을 적용하기 어렵다. 또한 양산 시에 테스트 시간은 제품 단가에 매우 중요한 요소로 작용하므로 본 연구에서는 각각의 테스트 루틴을 칩 내부에 미리 하드웨어 로직으로 구현하여 외부에서는 각각의 루틴에 대한 순서를 제어하고 그 결과만을 출력하여 비교할 수 있다. 그리하여 입.출력 데이터의 양을 획기적으로 줄여 테스트 시간을 단축하였다.

EEPROM을 위한 테스트루틴으로는 여러 가지 패턴 테스트(Write-all, Erase-all, Diagonal, Checker-board, Reverse-checker-board, Column-check)가 지원되는데 이는 서로 인접한 셀 간의 간섭효과를 검증한다. 그리고 에이징(Aging)테스트 항목으로 쓰기/지우기의 동작을 10,000번하고 그 이후의 셀의 기능상태를 점검한다.

칩이 지원하는 여러 가지 모드의 기능테스트로는 모드 및 스피드 테스트, 제조자 모드 테스트, TC 및 Lock 모드 테스트, 발행자 모드 테스트, 사용자 모드 테스트 등 크게 나누어 다섯 부분으로 구성되어 있다. 모드 및 스피드 테스트에서는 4가지 모드와 스피드에서의 기본적인 동작을 확인한다. 제조자 모드 테스트에서는 설계된 Lock-cell의 상태를 점검하고 EEPROM의 0-3 번지 영역에 데이터를 쓰고 확인하며 TC Lock 기능을 확인한다. TC 및 Lock 모드 테스트는 TC 및 Error Counter 즉 18-21번지 영역을 읽어서 기능을 확인하고 Lock 기능을 테스트한다. 발행자 모드 테스트에서는 EEPROM 쓰기 방지기능을 점검하고 발행자 영역의 데이터를 쓰고 검증하며 OTP Lock을 수행한다. 마지막으로 사용자 모드 테스트에서는 EEPROM 쓰기/읽기 방지영역에 대한 테스트를 하고 현금영역 쓰기와 인증 기능을 검증한다. 또한 사용자 영역에 대한 쓰기/읽기 테스트를 끝내고 최종적으로 다시 제조자 모드로 간다.

Ⅳ. 결 론

본 논문에서는 자체 테스트 및 보안기능을 갖는 공중전화 카드 IC의 구조를 제안하였다. 제안된 하드웨어는 기능 블록으로 내부에 EEPROM, 인증블럭, 보안회로, 간단한 제어기 등이 설계되어 외부의 단말기와 하나의 데이터 라인으로 비동기(혹은 동기) 통신에 의해 정보를 주고 받는다. 이러한 구조는 특히 테스트와 보안기능의 중요성이 논의되는데 본 연구에서는 이 점들을 다루었다. 외부와의 통신량을 줄이기 위하여 다양한 테스트 기능을 칩 내부에 구현하였으며 TC, E/S, OTP-Lock 등의 기능과 전압센서를 이용하여 EEPROM과 칩 동작의 신뢰도를 높였다.

참 고 문 헌

[1] Siemens, SLE4436 Preliminary Short Product Information Rev.1.1, 1993.

[2] International Standard Organization, ISO-7816, 1993.

[3] Douglas R. Stinson, "Cryptography: Theory and Practice," CRC Press, 1995.

[4] Alfred J. Menezes, Paul C van Oorschot and Scott A. Vanstone, "Handbook of Applied Cryptography," CRC Press, 1996.

[5] Mahdi Abdelguerfi, Burton S. Kaliski and Wayne Patterson, "Public-key Security Systems," IEEE Micro, pp.10-24, June, 1996.

저 자 소 개

朴 台 根(正會員) 第 36卷 C編 第 9號 參照
현재 가톨릭대학교 컴퓨터 전자공학부 교수