32 비트 저전력 스마트카드 IC 설계

김 승철[1], 김 원종[1], 조 한진[1], 정 교일[2]
한국전자통신연구원, 반도체.원천기술연구소[1],
한국전자통신연구원, 정보보호연구본부[2]
전화 : 042-860-6626 / e-mail: skimc@etri.re.kr

Design of 32 bits Low Power Smart Card IC

Seungchul Kim, Wonjong Kim, Hanjin Cho, Kyoil Jung
Electronics and Telecommunications Research Institute

Abstract

In this paper, we introduced 32 bit SOC implementation for multi-application Smart Card and described the methodology for reducing power consumption. It consists of ARM7TDMI microprocessor, 192 KBytes EEPROM, 16 KB SRAM, crypto processors and card reader interface based on AMBA bus system. We used Synopsys Power Compiler to estimate and optimize power consumption. Experimental results show that we can reduce power consumption up to 62 % without increasing the chip area.

I. 서론

스마트카드는 일반적으로 CPU와 메모리를 내장하여 자체 계산 능력을 갖는 IC 카드의 종류를 일컫는다. 이미 8비트 마이크로프로세서, 수 KB 이상의 실효성 있는 메모리를 내장한 스마트카드가 상용화되어 보안, 금융, 교통 등의 분야에서 널리 사용되고 있다. 근래에 이르러 IC 카드의 응용 분야가 더욱 다양화되고 카드가 처리해야 할 정보량이 급증함에 따라 카드에 내장되는 IC의 자체 계산 능력의 향상과 보다 높은 보안성이 요구되고 있다. 이에 대응하기 위해 고성능 마이크로프로세서와, 수 십 KB의 메모리, 암호프로세서 등의 하드웨어를 기반으로 하여 강력한 보안 특성을 갖는 카드용 운영체제를 탑재한 SOC(System On a Chip) 형태의 스마트카드용 IC를 필요로 한다.

본 논문은 멀티 응용에 유리하면서도 높은 보안성을 갖는 자바 카드 운영체제(Java Card OS, JCOS)의 탑재에 적합하고, RSA, ECC 등의 암호 알고리즘을 기반으로 한 공개키 인증 시스템에 적용될 수 있는 스마트카드용 SOC의 설계에 관한 것이다.

카드 SOC의 하드웨어 구성은 그림 1과 같다.

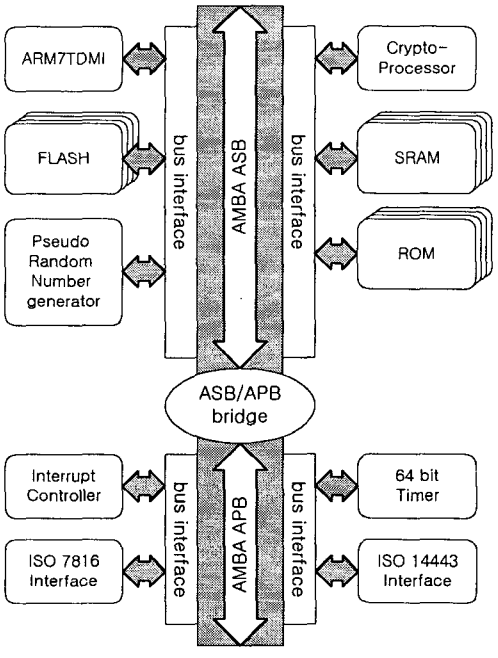

그림 3 . 스마트카드 칩 SOC 플랫폼

시스템 구성은 ARM사의 AMBA 버스 시스템을 기반으로 하였으며, ARM7TDMI 32 비트 마이크로프로세서와 208 KB 의 메모리, 타이머 등을 기본 구성으

로 한다. 공개키 인증 프로토콜 지원을 위한 요소로서 고성능 암호프로세서(한국전자통신연구원 정보보호연구본부)와 난수 발생기를 포함하고, 카드 단말(Card Reader)과의 인터페이스를 위한 회로 등으로 구성된다. 특히, 카드 단말 인터페이스 회로는 ISO 7816 접촉형 및 ISO 14443 비접촉형 카드 단말 규격 표준에 정의된 전송 프로토콜을 모두 만족하도록 하였다.

설계된 내용을 Epson의 0.35 um technology에 적용하였으며, Syopsys의 Power Compiler를 이용하여 소모 전력을 추정하였다. 소모 전력을 최소화하기 위해 Clock gating, Operand Isolation 등의 기법의 적용을 시도하였고, 그 결과를 기술하였다.

II. 스마트카드 SOC 설계

IC 카드의 주요 기술로는 다음의 4 가지를 들 수 있다.

- 카드 칩 설계 기술
- 카드 운영 체제(Card OS, COS) 기술
- 보안 기술
- 응용 서비스 기술

카드 칩 설계 기술이라 함은 데이터 처리를 위한 논리 회로 설계와 집적회로 제조 공정과 관련하여 요구되는 기술을 의미하고, COS 기술은 다양한 응용 서비스를 수용할 수 있기 위해 규모가 작으면서도 복잡한 제어 기능과 파일 관리, 보안 기능을 갖는 OS의 개발 기술을 의미한다. 보안 기술은 COS의 보안 특성을 포함하며, 소프트웨어와 하드웨어가 조합된 암호학적 측면에서의 안전성과 칩 외부로부터의 허용되지 않는 전기적, 물리적 접근을 막고 내부의 데이터를 보호하는 물리적 측면에서의 안전성을 보장하는 기술을 의미한다. 응용서비스 기술은 카드 단말기와 발행기 등의 인프라 구축과 각 응용 분야에 따른 애플릿 개발 기술 등을 의미한다.

카드 칩 설계 기술을 다시 카드용 CPU와 메모리, 암호 프로세서, 카드 단말 인터페이스 회로 설계, 각 요소 회로들을 연결하는 버스 시스템, 집적회로 제조 기술 등으로 나눌 수 있으며, 각 부분들에 대해 공통적으로 소모 전력의 최소화와 칩 면적의 최소화 문제가 고려되어야 한다.

2.1 AMBA 기반 설계

자바 가상 머신(Java Virtual Machine, JVM)이 포함된 JCOS를 탑재하고서 애플릿을 실시간으로 실행하기 위해서는 32 비트 급 이상의 고성능 마이크로프로세서를 필요로 한다. 이를 위해 저전력 특성이 좋고 32 비트와 16 비트 처리가 모두 가능한 ARM7TDMI 마이크로프로세서를 사용하였다.

메모리 구성은 128 KBytes의 JCOS 저장 영역과 실행 애플릿 및 카드 프로토콜 데이터를 저장할 64 KBytes의 비휘발성 데이터 영역, 4 KBytes의 RAM 영역으로 구성하였다. 추가적으로 칩 테스트를 위한 16 KBytes의 ROM이 삽입되었다. 실험적인 프로토타입 개발을 고려하여 OS 프로그램 영역을 비휘발성(Non-volatile) 메모리인 플래시 메모리로 구현하였다.

ARM 프로세서를 사용함에 따라 ARM 프로세서와 호환이 잘 되는 것으로 알려진 32 비트의 AMBA (Advanced Micro-controller Bus Architecture)를 기반으로 하여 스마트 카드 플랫폼을 구성하였다. ASB에는 버스 관리를 위한 기본적인 요소(어드레스 디코더, ARM7TDMI 코어 인터페이스 회로 등)들 외에 난수 발생 회로, 암호 프로세서, APB(주변유닛버스)와의 버스 확장 인터페이스 회로 등이 연결되어 있고, APB에는 인터럽트제어, 타이머, 접촉식 카드 단말기 인터페이스 (SCI), 비접촉 카드 단말기 인터페이스 (RFI) 모듈 등이 연결되어 있다.

암호 모듈로는 설계된 암호 모듈들의 기능을 검증하기 위하여 한 개의 RSA와 두 개의 ECC 알고리듬을 사용하였다. 1,024 비트 RSA, 차세대 비대칭 키 암호 알고리즘으로 알려진 타원곡선 암호 알고리즘 등을 고속으로 처리할 수 있는 암호 프로세서는 암호학적으로 안전성을 보장하는 키의 크기인 1,024 비트 이상의 공개키 RSA 알고리즘과 160 비트 이상의 Polynomial (Poly) 방식 의 타원 곡선 알고리즘을 수행하기 위해 독립된 두 개의 연산 블록으로 구성하였고, 한국전자통신연구원(ETRI) 정보보호본부의 1,024 비트 법(modular) 곱셈 연산기와 방식 타원곡선 암호/복호기를 사용하였다.

카드 단말 인터페이스 회로는 ISO/IEC 7816과 ISO/IEC 14443의 전기적 신호에 관한 규격을 만족하도록 설계하였다. 소프트웨어 설정에 따라 전송 속도를 조절 할 수 있으며, 접촉식의 경우 9600, 19200, 38400, 76800 bps, 비접촉식의 경우 106 kbps 송수신이 가능하도록 하였다.

2.2 시뮬레이션

설계된 SOC를 검증하기 위해 카드 단말 장치를 FLI (Foreign Language Interface)를 이용하여 모델링하였으며, 검증 환경을 그림 2에 나타내었다. SCI는 접촉식 카드의 동작을 검증하기 위한 것이며, RFI는 비접촉식 카드의 동작을 검증하기 위한 것이다. FLI 모

델은 데이터 파일로부터 필요한 명령 데이터를 접촉 또는 비접촉 인터페이스 프로토콜에 따른 입력을 제공하고, 카드 SOC로부터의 출력을 분석하여 프로토콜 오류나 명령 처리 결과를 확인한다.

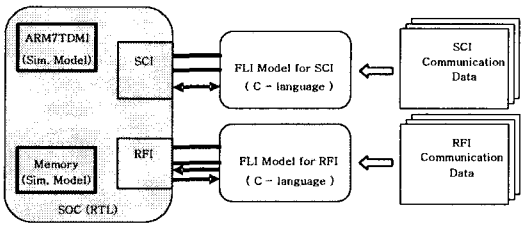

그림 4 . 시뮬레이션 검증 환경

2.3 소모 전력 추정

RTL 시뮬레이션 과정에서 도출된 칩 내부의 각 신호들의 스위칭 정보를 Synopsys의 Power Compiler에 적용하여 소모 전력을 추정하였다. RTL simulation에 사용된 테스트 벡터를 카드와 카드 단말 간의 실제 상황에 가깝게 묘사함으로써 실제 동작시의 소모 전력을 추정할 수 있도록 하였다. 하드 매크로 셀을 제외한 합성 회로에서의 소모되는 전력 중에서 암호프로세서가 대부분을 차지하는 것으로 나타났다.

표 1은 각각의 암호 모듈에 대하여 소모 전력을 추정 한 결과를 정리한 것이다. Cell Internal Power는 조합(Combinational) 회로와 순차(Sequential) 회로에서의 소모 전력의 합이며, 총 소모 전력(Total Dynamic Power)은 Cell Internal Power와 Net Switching Power의 합으로 계산된다.

표 2 . 암호모듈들의 소모 전력 (mW) 및 면적 (KG)

Algorithm	RSA	ECC1	ECC2
Cell Internal Power	265.3	94.6	44.8
- Combinational	134.8	10.2	14.8
- Sequential	130.5	84.4	30.0
Net Switching Power	302.9	159.4	163.7
Total Dynamic Power	**568.2**	**254.0**	**208.5**
Area (K Gates)	108.5	73.6	31.8

2.4 면적 및 소모 전력 최소화

ISO 7816에서 카드의 물리적 변형에 의한 내장된 칩의 손상을 막기 위해 카드용 IC의 크기를 25 mm2 이내로 할 것을 명시하고 있다. 또한 비접촉형의 경우, 카드 단말로부터 RF에 의해 유기되어 칩에 공급될 수 있는 전력은 수 십 mW에서 최대 200 mW 정도에 불과하다. 따라서 이러한 스마트카드의 특성상 소모 전력과 면적의 최소화는 RTL 설계 과정이나 합성/구현 과정에서 반드시 고려되어야 한다.

0.35 um 공정 기술을 적용하였을 때, 그림 3의 1차 레이아웃 결과와 같이 약 70 mm^2의 면적을 보였다. 여기서 COS용 Flash Memory를 ROM으로 대체하고, 암호 모듈의 수와 크기를 줄여서 0.18 um 공정 기술을 적용할 경우 25 mm^2에 근접할 수 있을 것으로 기대된다.

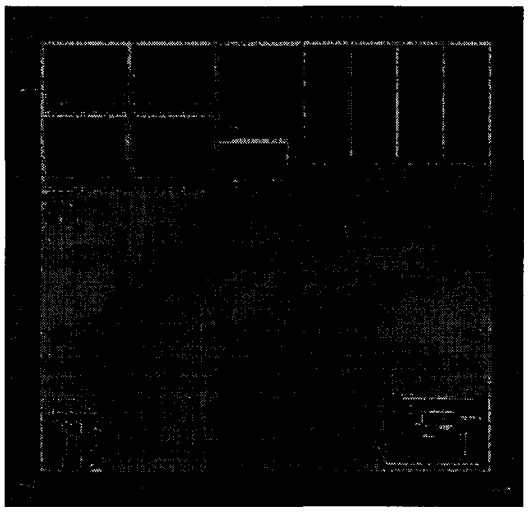

그림 5 . 스마트카드 칩 레이아웃

소모 전력 최소화는 RTL 수준에서 Sleep 모드 제어 회로를 첨가하는 방법과 특정 블록 내의 레지스터들에 불필요하게 공급되는 클록을 제어하여 연결된 각 노드에서의 스위칭 비율을 낮추는 방법을 함께 고려하였다. 후자의 경우 회로의 특성상 가장 많은 소모 전력 감소 효과를 얻을 수 있을 것으로 예상되는 Clock gating과 Operand isolation 기법을 적용하였다.

암호프로세서 내에 RSA 연산 회로와 ECC 연산 회로로 나뉘어지며, RSA의 경우에는 매 클럭마다 연산 회로가 동작하고, ECC의 경우 단순한 구조의 연산 회로로 구성되어 있어 두 가지 경우 모두 Operand Isolation의 효과를 얻지 못하였다.

그림 4 는 Synopsys의 Power Compiler와 Design Compiler를 이용하여 Clock gating을 적용하는 소모 전력 최적화 과정을 나타낸 것이다.

표 2는 clock gating을 적용하여 암호 모듈들의 소모 전력을 최소화한 결과를 나타낸 것이다. 전체 소모 전력과 면적에서의 백분율 값은 표 1의 결과를 100%로 하여 계산한 것이다. 표 1의 결과와 비교하면, RSA의

경우 별다른 차이를 보이지 않았으나, ECC는 각각 44.7%와 62.1% 소모 전력이 감소한 것을 볼 수 있다. RSA의 경우 대부분의 조합회로가 매 클럭마다 동작하는 구조로 설계되어 있기 때문에, 여러 가지 연산을 처리할 수 있도록 구성된 ECC에 비하여 소모 전력이 감소하지 않은 것으로 판단된다.

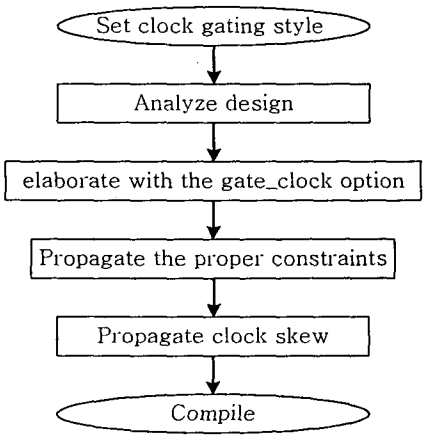

그림 6. Clock gating 컴파일

표 3 . Clock gating에 의한 소모 전력[mW] 최적화

Algorithm	RSA	ECC1	ECC2
Cell Internal Power	195.2	46.5	30.2
- Combinational	109.5	9.7	16.6
- Sequential	85.7	36.9	13.6
Net Switching Power	347.1	94.0	48.8
Total Dynamic Power	**542.3**	**140.5**	**79.0**
	95.5%	55.3%	37.9%
Area (K Gates)	92.6	64.9	29.2
	85.3%	85.1%	91.8%

Ⅳ. 결 론

본 논문은 자바 카드 운영체제(JCOS)의 탑재에 적합하고, 고도의 암호 알고리즘을 기반으로 한 공개키 인증 시스템에 적용될 수 있는 스마트카드용 SOC의 설계에 관한 것이다. 특히, 차세대 스마트카드의 핵심으로 각광 받고 있는 JCOS와 ECC 암호 알고리즘의 수용은 다양화되는 카드 산업에 적절히 활용될 수 있을 것으로 기대된다.

또한, 주요 전력 소모 요인인 암호프로세서의 설계에 Clock gating의 소모 전력 최적화 방법을 적용하여 ECC 알고리즘 수행에 소모되는 전력을 62% 까지 감소시킬 수 있었다.

참고문헌

[1] Jose Louis Zoreda and Jose Manuel Oton, "Smart Cards" Artech House, 1994.

[2] H.Dreifus and J.T.Monk, "Smart Cards: A guide to building and managing smart card applications", John Wiley & Sons, 1998.

[3] 손승원, "TM-0730-2000-010 : 차세대 IC카드 OS 개발", 한국전자통신연구원, 2000.

[4] 임영이, 이윤철, 강희일, 이동일, "스마트카드 기술동향", 주간기술동향, Oct. 1999.

[5] Mike Hendry, Smart Card Security and Applications, Artech House, 1997.