반도체설계교육센터
IC DESIGN EDUCATION CENTER

IDEC newsletter

VOL. 218
August 2015

IDEC Newsletter I 통권 제218 호
⊙ **발행일** 2015년 07월31일 ⊙ **발행인** 박인철 ⊙ **편집인** 남병규 ⊙ **제 작** 푸울디자인
⊙ **기 획** 석은주/김해리 ⊙ **전 화** 042) 360-8538 ⊙ **팩 스** 042) 360-8540 ⊙ **홈페이지** http://idec.or.kr
⊙ **E-mail** eunjuseok@idec.or.kr ⊙ **발행처** 반도체설계교육센터(IDEC)

반도체설계교육센터 사업은 미래창조과학부(산업통상자원부), 한국반도체산업협회, 반도체회사(삼성전자, SK하이닉스, 매그나칩반도체, TowerJazz코리아, 앰코테크놀러지코리아, ATI세미콘)의 지원으로 수행되고 있습니다.

IDEC newsletter

VOL. 218 August 2015

MPW (Multi-Project Wafer) 2015년 MPW 진행 내역

- 6개 공정 16회 진행, 2015년 MPW 모집 마감
- 2016년 진행 일정은 11월 이후 공지 예정
- 2015년 MPW 진행 일정 및 진행 내역

공정	회차구분 (공정_년도순서)	모집팀수 ((mmxmm)x칩수)/회별	정규모집 신청마감	참여팀수 ((mmxmm)x칩수)	DB 마감	Die-out	비고
삼성 65nm	S65-1501	(4x4) x48	2014.12.29	(4x4)x 39	2015.06.15	2015.12.14	DB 검토중
	S65-1502		2015.04.20	(4x4)x 29	2015.10.19	2016.04.19	설계중
	S65-1503		2015.06.22	(4x4)x 33	2016.01.18	2016.07.18	설계중
MS 0.18um	MS18-1501	(3.8x3.8) x25	2014.12.29	(3.8x3.8)x17 (3.8x1.9)x16	2015.03.02	2015.08.03	제작완료
	MS18-1502		2015.01.26	(3.8x3.8)x20 (3.8x1.9x7	2015.05.11	2015.10.12	칩제작중
	MS18-1503		2015.02.23	(3.8x3.8)x19 (3.8x1.9)x5	2015.07.13	2015.12.14	DB검토진행
	MS18-1504		2015.03.23	(3.8x3.8)x22 (3.8x1.9)x6	2015.09.07	2016.02.01	설계중
	MS18-1505		2015.05.26	(3.8x3.8)x24 (3.8x1.9)x2	2015.12.18	2016.05.09	설계중
MS 0.35um	MS35-1501	(5x4)x20	2015.01.26	(5x4)x18 (5x2)x3	2015.06.08	2015.09.29	설계중
	MS35-1502		2015.07.20	5x4)x19 (5x2)x2	2016.01.11	2016.04.30	설계대기
TJ SiGe	TJS18-1501	(2.35x2.35)x4	2014.12.29	(2.35x2.35)x1	2015.04.27	2015.09.15	제작지연
TJ CIS	TJC18-1501	(2.35x2.35) x4	2015.01.26	(2.35x2.35)x4	2015.06.15	2015.10.23	제작지연
	TJC18-1502		2015.05.26	(2.35x2.35)x4	2015.11.23	2016.03.28	설계중
TJ BCD	TJB18-1501	(2.35x2.35) x12~16	2014.12.29	(5x2.5)x2 (2.35x2.35)x8	2015.03.02	2015.07.06	제작완료
	TJB18-1502		2015.03.23	(5x2.5)x2 (2.35x2.35)x8	2015.08.24	2015.12.28	설계중
	TJB18-1503		2015.05.26	(2.35x2.35)x9	2015.11.30	2016.04.04	설계중

* 문의 : 이의숙 (042-350-4428, yslee@idec.or.kr)

* 일정은 사정에 따라 다소 변경될 수 있음.
* 회차 표기 방법 변경 : 공정코드-년도 모집순서 (예시) 삼성65nm 2015년 1회차 : S65-1501)
* TowerJazz 공정은 sub chip(2.35mmX2.35mm)으로 분리하여 모집
* 모집기간 : 모집 마감일로 부터 2주전부터 접수
* Package 제작은 Die out 이후 1개월 소요됨
* 기준일 : 2015. 07. 24

2015년 8월 교육프로그램 안내

수강을 원하는 분은 IDEC 홈페이지(www.idec.or.kr)를 방문하여 신청하시기 바랍니다.

개설 강좌 안내

센터명	강의일자	강의제목	분류
본센터	8월 3-5일	RF IC 설계 교육(1)	설계강좌
	8월 7일	Incisive Verilog Simulation	Tool강좌
	8월 10-13일	RF IC 설계 교육(2)	설계강좌
	8월 17-18일	Verilog HDL을 통한 Digital IP 구현	설계강좌
	8월 19-21일	AMBA AXI 기반 IP 설계와 검증	설계강좌
	8월 24-25일	디지털 신호처리를 위한 고성능 저전력 SoC 설계	설계강좌
	8월 28일	Encounter Digital Implementation	Tool강좌
경북대	8월 17-18일	아날로그 Front end 설계	설계강좌
	8월 20일	Low power SoC 설계 방법론	설계강좌
	8월 24-25일	안드로이드 플랫폼 설계 방법 및 하드웨어 제어 응용	SW강좌
광운대	8월 10-12일	스마트 모바일 AP기반 SoC구조 및 주변장치 응용	설계강좌
	8월 24-27일	Wearable Bio IoT	설계강좌
	8월 25-28일	IoT 시스템 및 보안 프로그래밍	설계강좌
부산대	8월 5-7일	Full Custom IC 설계	설계강좌
	8월 11-13일	Matlab을 이용한 Digital Signal Processing	Tool강좌
	8월 19-20일	SoC구조 및 설계	설계강좌
	8월 25-26일	고속 SoC platform 구현을 위한 PCB 설계이론	설계강좌
성균관대	8월 5-7일	RF 집적회로 설계 - RF 능동 /수동 소자 이해	설계강좌
	8월 12일	고속 시리얼 인터페이스 개요	설계강좌
	8월 13-14일	FPGA/ASIC, SoC 설계를 위한 HDL Coding 기법 강좌	설계강좌
	8월 17-19일	Synopsys Design Compiler 사용법 및 활용 예	설계강좌
	8월 20-21일	고성능 데이터 변환기 설계	설계강좌
	8월 24-26일	SoC설계이해 및 Synopsys IC Compiler 사용법 및 활용예	설계강좌
	8월 27-28일	ARM Cortex-M0 DesignStart를 활용한 SoC Platform 교육	SW강좌
전남대	8월 27-28일	mm 대역을 위한 PLL의 설계	설계강좌
	8월 11-13일	집적회로 설계의 기초	설계강좌
	8월 26-28일	Verilog HDL을 이용한 16bit 마이크로 프로세서 설계	설계강좌
	8월 26-28일	Verilog HDL을 이용한 16bit 마이크로 프로세서 설계	설계강좌
충북대	8월 5-7일	저잡음 operational amplifier설계 기법	설계강좌
	8월 6일	Verilog 설계 언어 초급	설계강좌
	8월 7일	Verilog 설계 언어 중급	설계강좌
	8월 24-25일	VLSI 테스팅	설계강좌

*문의 : KAIST IDEC 오가영 (042-350-8536, oky0818@idec.or.kr)

「 2016년 WG 」 선정 안내

IDEC은 "시스템반도체설계인력양성" 과 "핵심 IP 개발" 을 위하여 전국 대학의 교수들을 WG(Working Group) 참여교수로 선정하여 지원하고자 합니다.
많은 관심과 참여 바랍니다.

■ 지원내용

- 최신 기술 공정의 칩제작(MPW) 지원(Cell Library 포함)
- EDA Tool(26종) 지원
- IDEC 보유 Analog IP 지원
- 기타 IDEC의 다양한 자원 지원

■ 선정 일정

■ 온라인 작성 : http://idec.or.kr/ 로그인/ WG/ WG 성과 또는 WG 신청서 작성

■ 문의처 : Tel. 042-350-8533, E-mail : ejkim@idec.or.kr

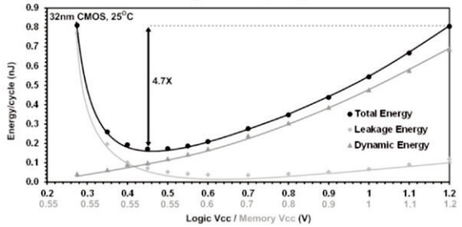
· 기존 및 신규로 선정된 참여교수는 선정 이후 3년간 실적이 없을 경우, 지원 중단

※ 자세한 사항은 IDEC 홈페이지(http://idec.or.kr)를 참고하여 주세요.

초저전력을 위한 Near-threshold Voltage SRAM 설계

1 Near-threshold Voltage 설계의 필요성

수년 전, 집적회로의 주요한 애플리케이션이 데스크탑 컴퓨터나 서버였다면, 현재는 스마트폰이나 태블릿 같은 모바일 기기들이 더욱 주요한 애플리케이션으로 각광받고 있다. 전문가들은 수년 뒤 사물인터넷, 웨어러블 컴퓨터 등이 집적회로의 주요 애플리케이션이 될 것을 예고하고 있다. 실제 각종 IT 회사들은 차기 전략 제품으로 스마트 시계를 출시한 바 있다. 사물인터넷의의 경우는 스마트 그리드를 위한 전기/가스/수도 등의 유틸리티 검침 분야를 비롯하여 환경 감시, 방범/방재, 공장/빌딩 자동화 및 시설제어, 구조물/기계부품 노후도 측정, 물류 관제, 국방, 농/축산, U-health등 다양한 분야에서 활용 범위가 지속적으로 확대될 가능성이 크다. 주목할 점은, 이러한 경향 속에서 배터리의 크기는 점점 축소될 수밖에 없으므로 집적회로에 허용되는 소모 전력의 크기도 크게 줄어들 수밖에 없다는 것이다. 그러므로 향후 집적회로 설계에 있어서 성능보다는 에너지 효율성이 더욱 중요해질 것임이 자명하다.



〈그림 1〉 공급 전압과 디지털 회로의 에너지 소모량과의 관계
(Intel사 발표 자료에서 발췌)

이러한 수요를 만족시키기 위하여, 학계에서는 집적회로의 에너지 효율성을 획기적으로 개선할 수 있는 기술들을 계속적으로 연구하였으며, 그 중 가장 각광받고 있는 기술이 Near-threshold Voltage (NTV) 회로 설계 기술이다. 〈그림 1〉은 디지털 회로의 공급 전압과 에너지 소모량의 관계를 보여주는 그래프로서, NTV 동작의 필요성을 잘 보여주고 있다. 디지털 회로의 에너지 소모량은 트랜지스터를 켜고 끄는 동작 과정에서 발생하는 동작 에너지(Dynamic Energy)와 동작 여부와 관계없이 흐르는 누설 전류에 의하여 소모되는 누설 에너지(Leakage Energy)의 합이 된다. 여기서, 동작 에너지와 누설 에너지는 각각 아래의 식 (1)과 (2)로서 표현될 수 있다. 주목할 점은 동작 에너지의 경우 공급 전압이 감소할 경우 감소량의 제곱만큼 줄어든다는 것이다.

하지만, 공급 전압 감소 시 회로의 지연 시간은 기하급수적으로 커지므로 clock 신호의 주기 역시 이에 맞추어 증가하게 된다. 이로 인하여, 〈그림 1〉에서 보듯이 누설 에너지는 공급 전압이 낮아질 경우 오히려 증가하게 된다. 결과적으로 공급 전압을 낮출 경우 전체 에너지 소모량은 처음에는 감소하지만, 어느 지점부터는 오히려 증가하는 현상이 일어난다. 이는 공급 전압 변화 시 에너지 최저점이 존재한다는 뜻이며, 〈그림 1〉에서 보듯이 그 최저점은 트랜지스터의 문턱전압 근처인 400~600mV 부근에서 나타난다. 즉, NTV에서 회로를 동작 시킬 경우 우리는 집적회로의 에너지 효율을 최적화하는 것이 가능하다. 실제 인텔사는 NTV 회로 설계 기술을 활용하여 집적회로의 전력 소모량을 획기적으로 개선하려는 계획을 발표한 바 있다.

$E_{dynamic} = \alpha CV^2$ (α : 개폐 동작 횟수, C: 회로의 부하 정전 용량, VDD:공급 전압) (1)

$E_{leakage} = \int_0^{T_{CLK}} i_{leak} VDD dt \propto CV^2$ (ileak: 누설전류, T_{CLK}: clock 신호 주기) (2)

2 Near-threshold Voltage SRAM 설계의 기술적 장벽

NTV 동작을 활용할 경우 에너지 효율성을 크게 개선할 수 있지만, 많은 문제점 또한 발생한다. 무엇보다 트랜지스터 전류가 NTV와 같은 저전압에서는 공정, 온도, 전압 등의 변이에 극히 민감해지기 때문에 하드웨어의 동작 신뢰성이 크게 저하될 수밖에 없다. ARM사는 2015년 ISSCC에서 NTV 영역에서 동작하는 프로세서를 발표하면서, 극복해야할 기술적 장벽 및 난이도를 간략히 정리하여 발표한 바 있다 [1] (〈그림 2〉 참조).

〈그림 2〉 NTV 회로 설계의 주요 기술적 장벽과 난이도
(출처: ARM사 2015년 ISSCC 발표자료)

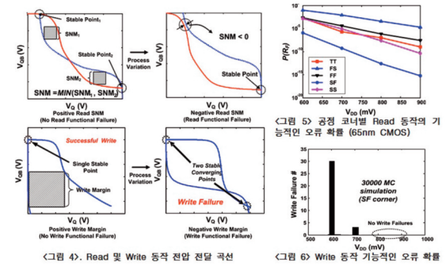
이에 따르면, NTV 회로 설계 시 가장 어려운 기술적 장벽은 NTV에서 동작하는 내장형 메모리인 SRAM을 설계하는 일이다. SRAM의 NTV 동작이 어려운 이유를 정리하면 아래와 같다.

〈그림 3〉 6T SRAM 셀 구조

가. 높은 기능적 오류 발생 확률

〈그림 3〉은 6T SRAM의 구조를 보여준다. 이 6T SRAM 셀의 읽기 및 쓰기 동작 바이어스 상황에서 메모리 노드중 하나를 특정 전압으로 강제할 경우, 다른 노드의 출력을 관찰하면서 그린 것이다. 이러한 곡선을 SRAM 셀의 전압 전달 특성 곡선이라 부른다. SRAM의 읽기 동작 시 메모리 노드에 어느 정도의 노이즈가 발생하는 것은 불가피하다. 그럼에도 불구하고, 저장한 데이터를 보존하기 위해서는 전압 전달 특성 곡선에 2개의 안정적인 수렴점이 존재해야 한다. 하지만 공정 또는 온도 변이로 인하여 수렴점이 1개만 존재하는 경우가 발생하며, 이 때 해당 SRAM 셀은 읽기 동작 중 기능적인 오류가 발행한다.

읽기 동작과는 달리 SRAM 셀이 성공적인 쓰기 동작을 수행하기 위해서는 〈그림 4〉의 좌측 하단 그림처럼 수렴점이 1개만 존재하여야 한다. 하지만, 공정과 온도 변이 시 여전히 2개의 수렴점이 존재할 수도 있으며, 이 경우에는 성공적으로 쓰기 기능을 수행할 수 없다. 이러한 기능적인 오류들은 해당 SRAM 셀에서는 같은 오류가 반복적으로 발생하므로, 집적회로의 수율에 직접적인 영향을 끼친다. 〈그림 5〉와 〈그림 6〉은 65나노 CMOS공정에서 공급 전압을 변화시킬 경우, 위와 같은 오류들이 발생할 확률을 시뮬레이션을 통하여 예측한 것이다. 여기에서, 우리는 공급 전압이 낮아질수록 오류가 발생할 확률이 기하급수적으로 커지는 것을 볼 수 있다. 이는, NTV에서 SRAM 읽기/쓰기 동작 중 발생하는 기능적인 오류 발생 확률이 매우 크다는 것을 의미한다.



〈그림 4〉. Read 및 Write 동작 전압 전달 곡선

〈그림 5〉 공정 코너별 Read 동작의 기능적인 오류 확률 (65nm CMOS)

〈그림 6〉 Write 동작 기능적인 오류 확률

나. 동작 전류와 누설 전류간의 차이 감소로 인한 센싱 오류 확률 증가

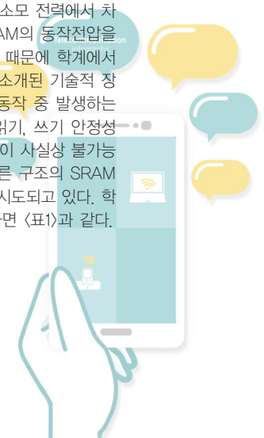
6T SRAM에서는 두 bit-line(〈그림 3〉의 BL과 BLB)을 공급 전압만큼 충전한 후, 저장된 데이터에 따라 한 bit-line만 방전되도록 한다. 이상적으로는 오직 한 bit-line에 저장된 전하만이 동작 전류에 의해 방전되어야 하지만 다른 bit-line에 충전된 전하 역시 누설 전류로 인하여 어느 정도 방전되는 것은 피할 수 없다. 그럼에도 불구하고, 일정 시간 후 동작 전류와 누설 전류로 인한 방전 정도의 차이를 이용하여 저장된 데이터를 센싱할 수 있다. 그런데, 공급 전압이 낮아질 경우 트랜지스터의 동작 전류와 누설 전류의 차이는 기하급수적으로 줄어든다. 즉, 유사 문턱 전압에서는 동작 전류와 누설 전류의 차이가 매우 작아지며 이러한 상황에서 공정 또는 온도 변이가 발생할 경우 센싱 동작 도중 오류가 발생할 수 있다.

다. 소프트 에러에 취약

그 외에도, SRAM이 소프트 에러에 노출될 확률이 증가할 수 있다 [2]. 전압이 낮아질 경우, 메모리 셀 데이터를 뒤집기 위하여 요구되는 최소 전하량(Qcrit)은 비례하여 줄어든다. 이로 인하여, 한 번의 소프트 에러 발생 시 데이터 오류가 발생하는 메모리 셀의 개수도 늘어날 개연성이 크다. 이러한 문제점을 Multiple Event Upset(MEU)이라고 하며, NTV 영역에서는 SRAM에서 발생하는 MEU에 대한 대비책이 필요하다.

3 대표적인 연구 결과들

SRAM을 NTV에서 안정적으로 동작시키는 것은 위와 같은 기술적 장벽들로 인하여 매우 어려운 것이다. 이 때문에, NTV관련 연구를 진행하는 대부분의 기업들은 조합/순차논리 회로 대비 SRAM의 공급전압은 다소 높은 영역을 활용하는 방향으로 연구를 진행 중이다. 하지만, SRAM의 소모 전력이 전체 집적회로 소모 전력에서 차지하는 비중에 매우 크다는 점을 고려할 때, SRAM의 동작전압을 공격적으로 스케일링하는 것은 매우 중요하다. 이 때문에 학계에서는 관련 연구를 계속적으로 진행 중이다. 위에서 소개된 기술적 장벽들 중 가장 극복이 어려운 부분은 읽기, 쓰기 동작 중 발생하는 높은 기능적 오류 확률이다. 6T SRAM 구조는 읽기, 쓰기 안정성이 서로 상반관계이므로 이를 동시에 극복하는 것이 사실상 불가능하다. 이 때문에, 트랜지스터의 개수를 추가한 다른 구조의 SRAM을 이용하여 이를 극복하려는 노력이 지속적으로 시도되고 있다. 학계에 발표된 대표적인 연구 성과를 간략히 요약하면 〈표1〉과 같다.



[표 1] SRAM 공급 전압의 공격적인 스케일링과 관련된 대표적인 연구 결과

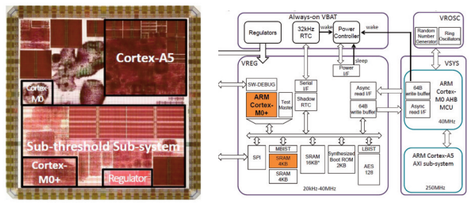
구 분	Single-end 8T cell	Single-end 10T cell	Differential-end 10T cell
최초 발표	VLSI Symp.	ISSCC 2006, JSSC 2007	ISSCC 2008, JSSC 2009
발표기관	IBM	MIT	Purdue

위 SRAM들의 공통점은 6T SRAM과는 달리, 읽기 동작을 위한 buffer를 두고 있다는 것이다. 이 buffer로 인하여 읽기 동작 동안 SRAM의 메모리 노드들인 Q와 QB는 bit-line의 접근으로 인하여 발생하는 노이즈로부터 자유롭다. 이는 읽기와 쓰기 안정성을 동시에 개선하는 것을 가능하게 한다.

위 연구 결과 중 IBM에서 발표한 Single-end 8T SRAM [3]은 상용화에 성공하여, 현재 일부 CPU의 내장형 메모리에 실제 사용 중이다. Single-end 10T SRAM [4]은 Single-end 8T SRAM 대비 센싱 안정성을 크게 개선하였지만, 넓은 면적 비용으로 인하여 실제 상용화까지 연결되지는 못하였다.

Differential-end 10T SRAM[5]은 본 저자가 Purdue대학 재학 시절 제안한 것으로서, 기존의 Single-end 8T/10T SRAM 대비 두 가지 점에서 큰 장점이 있다. 첫 번째는, Differential 구조를 활용하여 Single-end 구조 대비 센싱 안정성을 크게 개선하는 것이 가능하다. 두 번째는, Single-end 8T/10T SRAM은 메모리 쓰기 동작 중 인접 셀들의 동작 안정성이 위협 받기 때문에 bit-interleaving 구조를 취하는 것이 어렵지만, Differential-end 10T SRAM은 그러한 문제점이 없으므로 bit-interleaving 구조로 구현이 가능하다.

Bit-interleaving 구조는 위에서 언급한 세 번째 기술적 장벽인 MEU문제를 효율적으로 극복하기 위하여 반드시 필요하다. 하지만 넓은 면적 비용으로 인하여 아직 상용화에 성공하지는 못하고 있다. 하지만, 현재 ARM사의 경우 NTV 동작에 가장 적합한 SRAM으로 이 Differential-end 10T SRAM을 지목하여 현재 연구를 진행 중이며, 실제 2015년 ISSCC에 이 SRAM을 이용한 NTV동작 프로세서 시제품을 개발하여 발표하였다 (<그림 7> 참조). ARM사는 자신들이 개발한 프로세서가 NTV보다 더욱 공격적으로 전압을 스케일링한 Sub-threshold 영역에서도 성공적으로 동작한다는 것을 증명하였다.



<그림 7> 2015년 ARM사가 발표한 NTV동작 프로세서 시제품의 레이아웃 및 구조

④ 결론

지금까지 NTV 영역에도 동작하는 SRAM 설계의 기술적 장벽 및 대표적인 연구 결과를 간략히 정리하여 기술하였다. 이와 관련한 연구들은 현재도 활발히 학계에서 진행 중에 있으며, 그 결과들이 국제 저널 및 학술대회에서 발표되고 있다. NTV SRAM 설계는 NTV 집적 회로 설계 중 가장 어려운 부분이지만, 관련 기술이 축적될 경우 상용화에도 성공하는 기술이 개발될 것으로 기대한다. 이는 상용화에 성공한 NTV 집적회로의 출현을 의미하며, NTV 집적회로 설계 기술의 성공은 사물인터넷과 웨어러블 컴퓨터의 가장 큰 문제점인 짧은 배터리 문제를 획기적으로 개선하는 출발점을 제공할 것이라 확신한다.

장 익 준 교수
소속 : 경희대학교 전자전파공학과
주 연구분야 : NTV 회로 설계, Approximate/Stochastic Computing에 기반한 video 관련 하드웨어 설계, 위성탑재를 위한 Radiation에 내구성을 가진 하드웨어 설계
E-mail : ichang@khu.ac.kr
Homepage: http://vlsi.khu.ac.kr/

참고문헌

[1] James Myers, Anand Savanth, David Howard, Rohan Gaddh, Pranay Prabhat, David Flynn, "An 80nW retention 11.7pJ/cycle active sub-threshold ARM Cortex-M0+ sub-system in 65nm CMOS for WSN applications", ISSCC, Feb, 2015

[2] C. Lage et al., "Soft error rate and stored charge requirement in advanced high-density SRAMs," IEDM Tech. Dig., Dec. 1993

[3] L. Chang, R. K. Montoye, K. A. Batson, R. J. Eickemeyer, R. H. Dennard, W. Haensch, D. Jamsek, "An 8T-SRAM for Variability Tolerance and Low-Voltage Operation in High-Performance Caches", Journal of Solid-State Circuits, Vol. 43, No. 4, pp 956-963, April 2008

[4] B. H. Calhoun and A. Chandrakasan, "A 256 kb sub-threshold SRAM in 65 nm CMOS," IEEE J. Solid-State Circuits, vol. 42, no. 3, pp. 680-688, Mar. 2007

[5] I. J. Chang, J. Kim, S. P. Park, K. Roy, "A 32kb 10T Sub-threshold SRAM Array with Bit-interleaving and Differential Read Scheme in 90nm CMOS", Journal of Solid-State Circuits, Vol. 44, No. 2, pp 650-658, Feb. 2009

반도체설계교육센터
IC DESIGN EDUCATION CENTER

2015
IDEC SoC Congress

일시 : 2015. 09.22(화) 09:40~19:00
장소 : KAIST KI빌딩 1층

대학에 설계 연구 환경 지원에 대한 결과를 소개·전시하고 대학과 관계자 분들과 함께 SoC 설계 인력 양성의 현안과 발전 방향에 대해 논의하고자 IDEC SoC Congress(ISC)를 개최합니다. 본 행사를 통해 산업의 근간인 인력양성에 대한 의견를 수렴하여 더욱 나아진 연구 및 교육 환경이 구축될 수 있도록 관계자 여러분의 많은 관심과 참여 부탁 드립니다.

› 진행 프로그램

- 성과전시 : MPW 설계 결과 전시(CDC)
- 최신 동향 세미나 : SoC 및 차량용 반도체의 기술 동향과 비전
- 포럼 : SoC 인력양성을 위한 대학 교육(기업-정부-대학)
- IDEC 수행 사업 보고 및 관련 시상

› 진행 일정

구분	Session1(강당,1F)	Session2 (로비,1F)
09:40~10:00	Registration	10:00 ~ 16:00 [IDEC 성과 전시] CDC참여팀 설계 우수팀
10:00~10:30	Opening - 축사(강성모 총장 , KAIST)	
10:30~11:50	[최신 동향 세미나] 차량용 반도체의 기술 동향 및 비전 (Kent.chon 사장, IT코리아)	
11:50~13:00	점심식사(패컬티 클럽)	
13:00~14:20	[최신 동향 세미나] SoC 산업의 기술동향과 비전 (이손석 부사장, 오보브반도체㈜)	
14:20~15:00	Break Time_관람전시	
15:00~15:30	[사업내용 보고 및 시상] - IDEC 사업 수행 내용 및 성과 발표 - CDC 우수팀 및 우수 강사 시상	
15:30~17:30	[포럼] - 참석: 대학-기업-정부 - 주제: SoC 인력양성을 위한 대학 교육 방향, IDEC 역할	
17:30~19:00	저녁식사(영빈관)	

• 주 최 : 미래창조과학부, 산업통상자원부
• 주 관 : 반도체설계교육센터(IDEC), KAIST
• 문의처 : 042-350-4428, http://idec.or.kr, yslee@idec.or.kr

FPGA Security

1. Introduction

최근에 반도체 공정기술이 점차 발전하면서 블루투스 장비(Bluetooth transceiver)에서부터 나사의 화성탐사 로봇에 이르기까지 임베디드 시스템에서의 FPGA의 사용이 점점 늘어나고 있다. 과거에는 FPGA가 미리 설계된 규칙적으로 배열된 논리 블록을 이용하여 구현해야 하기 때문에 주문형 반도체 보다 성능 면에서 제한적이었지만 최신의 공정기술들이 적용된 FPGA들에서는 ASIC과 비슷한 성능을 낼 수 있게 되었고, FPGA를 이용한 하드웨어 개발기간이 짧다는 장점들로 인해 그 이용빈도가 점점 늘어나게 되었다.

FPGA는 성능 면에서의 향상뿐만 아니라 동적 부분 재구성 방법(Dynamic Partial Reconfiguration)을 이용하여 실제 동작할 때 오류가 발생하는 부분만 재 수정할 수 있으며, 초기 개발비 또한 저렴하다. 그리고, 무엇보다도 현재 많은 임베디드 제품이 HW/SW 통합설계 방식을 이용해 설계 되어짐을 고려한다면, FPGA의 설계 유연성은 FPGA가 이처럼 인기를 얻는 요인으로 크게 작용했다고 할 수 있겠다. 이와 같이 FPGA의 많은 장점들로 인해서, 현재 기반시설, 통신장비(etc. WPA) 등 다양한 분야에서 사용됨과 더불어 관련 기술의 발전도 꾸준히 이루어지고 있다.

하지만, 이렇게 FPGA의 사용량이 늘어남에도 불구하고, FPGA에서의 보안 문제에 대한 인식은 많이 부족한 형편이다. 사실 임베디드 장비에 대한 보안 문제는 FPGA가 주로 ASIC칩을 제작하기 위한 시제품(prototype)을 제작하는 선에서 이용되었기 때문에 과거에는 주로 ASIC 칩에 대한 보안 해결책을 마련하는데 초점이 맞춰져 있었고, 2000년대에 들어서서야 FPGA에 대한 보안 취약점을 찾기 시작하였다. 따라서, 아직까지 FPGA에서의 많은 보안 문제에 대한 해결책이 마련되지 않았기 때문에, 현재 FPGA security에 대한 연구가 많은 관심을 받고 있다. 특히, 최근에는 FPGA의 늘어나는 수요로 인해서 FPGA에 탑재된 핵심 정보 기술을 착취하거나 불법 복제 및 서비스 거부 공격 등의 위협에 노출되는 보안 문제가 큰 사회적인 이슈로 떠오르고 있다. 따라서, 보안적인 관점에서의 FPGA 연구는 필수적인 요소가 되고 있으며, 향후 하드웨어에 대한 안전성 분석에 있어서 FPGA security가 중요한 이슈 중 하나로 각광 받을 것이다

본 칼럼에서는 대표적인 FPGA 보안 위협들과 이에 대하여 현재 상용화되고 있는 FPGA에 적용되어 있는 방어기법을 간략히 소개하고자 한다.

2. Classification & Structure of FPGA

FPGA는 SRAM 기반의 제품, 플래시 메모리, 그리고 안티퓨즈 기반의 제품이 있고, 어떤 특성의 메모리로 구성이 되었느냐에 따라 크게 휘발성 FPGA와 비 휘발성 FPGA 두 가지로 분류된다. 특히, 최근에는 재 프로그램이 용이한 점 때문에 SRAM 기반의 휘발성 FPGA 제품이 시장 점유율의 대부분을 차지하고 있다.

SRAM 기반의 FPGA는 전원공급이 차단되면, 휘발성 특징을 가지고 있는 SRAM으로 인해서, 내부 구성이 삭제되고 그 디자인은 사라진다. 따라서, 현재 거의 모든 FPGA 제품들은 전원을 공급할 때 마다 EEPROM이나 플래시 메모리와 같은 외부 부트 디바이스에 비트스트림(bitstream) 파일을 저장하여 놓고 전원을 공급할 때마다 FPGA를 재구성하는 방식으로 동작한다. 그림 1은 각 FPGA들을 구성하는 메모리 종류들을 나타내었다.

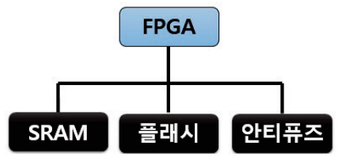


그림 1. 각 FPGA들을 구성하는 메모리 종류들

FPGA의 내부는 CLB라고 불리는 재구성 가능한 논리 블록 들과 이들 회로 블록간의 연결을 지원하는 채널 등으로 구성된다. 그림 2는 일반적인 FPGA의 내부 구조를 보여준다. 자일링스(Xilinx) 사의 Virtex FPGA 구조에서 일반적으로 CLB는 두 개의 Slice 또는 네 개의 Slice를 포함한다. 하나의 Slice는 다수의 LUT(Lookup Table)와 메모리(register) 소자로 구성된다.

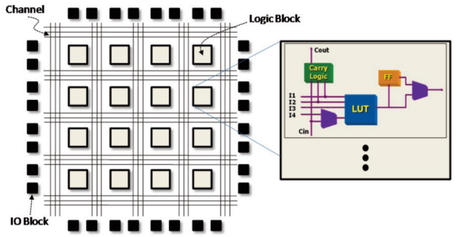


그림 2. 일반적인 FPGA의 내부 구조

그림 3과 같이 최신 FPGA는 이전 FPGA가CLB(Configurable Logic Blocks)와 Block Memory 구성으로만 되어있는 구조와는 다르게 미세 공정기술의 발달과 더불어 여러 기능이 집적되고 있다. 즉, ADC, DSP 블록과 같은 기능 제공은 FPGA의 활용범위를 넓히고 있으며, 특히 최근 자일링스 FPGA Family의 Zynq 시리즈의 경우 하드코어 프로세서(CPU)가 내장되어 있어, HW/SW co-design 형태의 설계에도 강점을 보이는 FPGA로 진화하고 있는 추세이다.

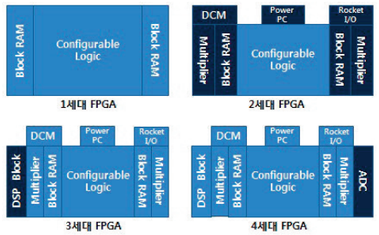


그림 3. FPGA의 구조상의 변화

3. FPGA Attack

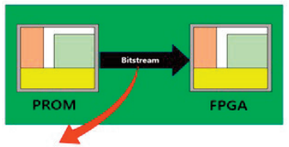


그림 4. 외부 메모리와 FPGA사이에서의 비트스트림 노출

FPGA에 대한 공격의 위험성은 그림 4와 같이 공격자가 FPGA를 재구성하기 위해 사용하는 외부 메모리들 간의 통신시 비트스트림 파일에 대한 데이터 탐침 공격(Probing attack)이 가능함으로 인해서 발생한다. 이뿐만 아니라, FPGA에 대한 공격은 복제(Cloning), 역공학 공격(reverse engineering), 서비스 부정(service denial)과 같은 다양한 방법들을 이용해 보안상 취약점이 드러나게 한다.

본 절에서는 대표적인 FPGA에 대한 공격 형태에 대해 간단히 설명하고, 각 공격방식에 대한 특징을 설명한다.

3.1 Cloning Attack

Cloning Attack은 FPGA에 내장되어 있는 디자인의 내용 자체는 요구하지 않고, 장비에 대한 복제에만 의의를 두는 공격이다. 예를 들면, 공격자가 FPGA에 들어갈 비트스트림 파일이 저장되어 있는 PROM의 내용을 수정하지 않고 그대로 불법 복제하여, 본래의 제품화되는 것과 동일한 사양의 장비에 적재하여 다시 파는 형태이다. 장비자체를 복제하는 것 이외에도 라이선스 비용을 부과하는 소프트코어의 비트스트림 파일을 로열티 없이 사용할 목적으로 무단 탈취 또는 불법 다운로드 하는 것도 이 공격에 해당한다.

그림 5. FPGA를 사용하는 시스코 라우터와 복제장비인 중국산 치스코 라우터

3.2 Bitstream Reverse Engineering Attack

역공학이라는 용어는 완성된 하드웨어 제품으로부터 설계정보를 해석해내는 분석기법으로부터 유래되었다. 그리고, 넓은 범위에서의 역공학은 완제품으로부터 분석 및 설계, 구현 단계들과 관련된 정보를 해석 및 분석하는 기법을 말한다.

FPGA에서의 비트스트림 역공학 공격이란, 가독이 불가능하게 인코딩된 이진파일 형태의 디자인(bitstream file)을 공격자가 해독 가능한 설계 언어(HDL) 형태의 디자인 파일로 복구하는 방법을 말한다. 공격자는 역공학 과정에서 HDL 설계언어 형태의 자세한 기능적 묘사 정보뿐 아니라, 구현된 FPGA 셀의 배치정보 및 경로정보(Place & Route)까지 얻어낼 수 있다. 그림 6은 FPGA 디자인 합성을 위해 컴파일러에 의해 생성되는 비트스트림 파일의 출력과정을 보여준다. 공격자는 그림 6의 좌측 화살표와 같이 역공학 과정을 통해 비트스트림 파일을 소프트 IP(HDL) 혹은 netlist 수준으로 되돌림으로써 설계에 대한 비밀정보(security key) 및 핵심적인 설계 아이디어(core circuit)를 탈취할 수 있다.

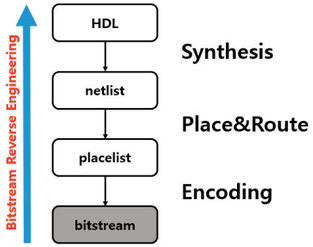


그림 6. 비트스트림 역공학

3.3 Tampering Attack

Tampering Attack은 공격자가 어플리케이션의 디자인을 무단으로 수정하는 공격을 말한다. 세부적으로는, 공격자의 역공학 공격 기법 보유 여부에 따라 다음과 같이 패치(Patch) 공격과 서비스 거부(Dos)공격 두 가지의 보안 위협으로 나타날 수 있다.

첫째, 공격자가 역공학 기법을 보유하고 있을 경우 공격자가 디자인 파일 구조를 수정할 수 있어 그 논리적 흐름에 직접 영향을 줄 수 있다는 점이다. 예를 들면 비밀 키와 같은 중요 정보를 누출할 목적으로 특수한 논리로직을 추가하는 기술인 패치(Patch)가 이에 해당된다.

둘째, 공격자가 완벽한 역공학 기법을 보유하고 있지 않더라도 장비 자체를 통제불능으로 만들어 서비스를 불가하게 하기 위한 목적의 공격이 가능하다. 이와 같은 공격을 서비스 거부 공격 (Denial of Service)라고 한다. FPGA의 서비스 거부 공격은 ROM에 저장되어 있는 비트스트림 파일 안의 내용을 뒤엉켜 놓는 것만으로도 가능하다. 특히 SRAM 기반 FPGA에 의존하는 상용네트워크 장비는 서비스 거부 공격에 노출되기 쉽다.

공격자는 FPGA의 비트스트림 파일에 접근함으로써 장비를 망가뜨리고 네트워크를 마비시킬 수 있게 된다. 또한 역공학 기술을 보유한 공격자는 장비 자체를 제어하기 위해 FPGA를 다시 재구성함으로써 더 큰 문제도 일으킬 수 있다. 예를 들면 통신 네트워크에서 해커는 카드 결제 알고리즘을 바꿔서 고객들이 금액 지불을 못하게 하거나, 공격자가 바이러스를 FPGA 기반의 네트워크 장비에 침투시켜 네트워크 전체에 이를 퍼뜨릴 수 있는 가능성이 있다.

4. Security methods for FPGA

본 절에서는 앞서 나온 공격 방법들에 대한 보안 방법론을 비밀키 생성, 비트스트림 파일의 암호화 및 복호화, 무결성 인증 방법론, 물리적 복제 방지 측면에서 설명하고, 현재 상용화되고 있는 FPGA들에 적용되어 있는 보안기법을 소개하고자 한다.

4.1 비밀키의 생성과 보호

비밀키(security key) 스토리지에는 암호화된 비트스트림 파일을 복호화 하는데 필요한 키 정보가 저장된다. 이 비밀키가 노출되면 비트스트림 파일을 가독 가능한 설계 언어로 변환이 가능함으로, 일반적인 FPGA의 경우 물리적 접근제어(access control)를 함으로써 보안성을 유지하고자 한다. 즉, 비밀키 스토리지의 정보는 주변 장치(PC 또는 노트북)에서 업로드(upload)는 가능하지만 읽기(read)는 불가능한 특징을 가진다.

상용 FPGA의 키 생성 과정의 경우, FPGA 벤더에서 제공되는 개발도구에 포함되어 있는 비트스트림 파일 생성기(e.g. Xilinx의 BitGen)에서 소프트웨어 의사 난수 생성기(Pseudo Random Number Generator)를 이용하여 비트스트림 암호화 키를 생성한다. 또한 앞서 생성된 동일한 비밀키가 FPGA 내부의 비밀키 저장 전용 스토리지에 JTAG을 이용하여 업로드 되어 복호화 키로 사용되는 방식이 일반적이다.
FPGA 내부의 비밀키를 저장하기 위한 스토리지는 휘발성 BBRAM(배터리 내장형 메모리)와 비휘발성 eFuse가 대표적이며, 그 형태에 따라 각각 장단점을 가진다. 아래의 표는 휘발성 BBRAM(배터리 내장형 메모리)와 비휘발성 eFuse 각각의 두 대표적인 스토리지에 대한 장단점을 나타내었다.

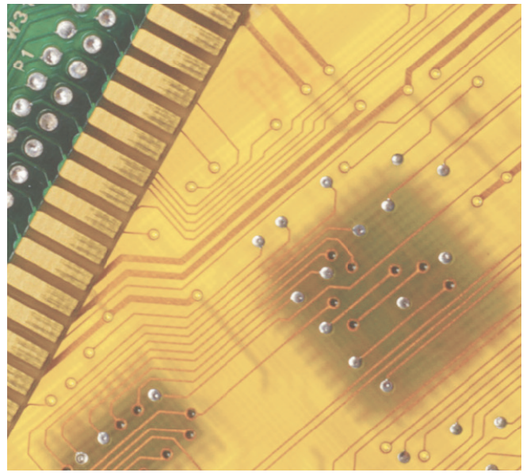
표 1. 키(key) 스토리지 형태에 따른 장단점

구분	BBRAM	eFuse
장점	• 휘발성재프로그램이 가능 • 탬퍼링 공격 저항성 • 물리적 완전 삭제 가능 - 증거가 남지 않음	• 베터리가 필요없음 • 스푸핑(Spoofing)공격이 불가
단점	• 베터리가 필요함 • 높은 온도에서 견디지 못함	• 키(key) 재 프로그램이 불가 • 삭제 자체가 안됨 • 노출됐을 경우 보안에 취약

키 스토리지에 있는 키 자체를 물리적 공격으로부터 안전하게 보호하기 위해서 Xilinx 및 ALTERA는 추가적인 보안 기법을 이용한다. 대표적인 키 스토리지 보호 방법 중 한 가지 방법은 키스토리지를 메탈레이어(Metal Layer) 아래에 분산적으로 설계해 놓는 방식이 있다.

4.2 비트스트림 암호화 및 복호화

휘발성 FPGA의 경우 외부 비 휘발성 메모리에 기록된 디자인 정보의 불법적인 탈취를 방지하기 위해 그림 7과 같이 암호화된 비트스트림 파일을 비휘발성 메모리(PROM)에 저장한다. 그리고, 전원이 공급되어 자동적으로 재 프로그래밍될 시 FPGA 칩 안에 내장되어 있는 복호화 회로가 암호화된 비트스트림 파일을 복호화 해주고, FPGA 구성 메모리(SRAM)로 업로드 됨으로써, 암호화/복호화를 이용해 비트스트림 파일 보호 한다.



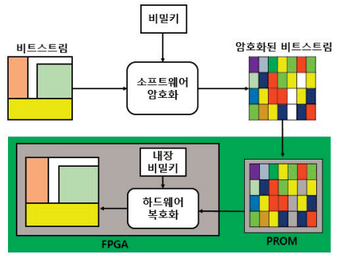


그림 7. 비트스트림의 암호화 방법

비트스트림의 암호화 과정은 FPGA 설계도구에 포함되어있는 비트스트림 파일 생성기(eg. Xilinx 의 BitGen)를 이용하여 암호화를 수행한다. FPGA 내부의 복호화 로직회로에는 DES (Data Encryption Standard)나 AES (Advanced Encryption Standard)와 같은 상용 표준 블록 암호 알고리즘을 처리하는 회로를 사용하며, 이 부분은 FPGA 내부의 프로그램이 가능한 일반 구성요소와 달리 공정 제조과정에서 FPGA 내부에 고정된 회로로 구현되며 사용자의 접근이나 변경이 불가능하다.

이러한 암호화 및 복호화를 통한 현행 FPGA 제품들의 비트스트림 파일 보호 방식은 공격자가 회로의 자세한 기능적 묘사 정보 획득하거나(Bitstream Reverse Engineering Attack) 복제공격(Cloning Attack) 으로부터 데이터를 보호하는 방식으로 비트스트림 파일에 대한 높은 수준의 비밀(confidentiality) 기능을 제공한다. 하지만, 그럼에도 불구하고, 최근에는 부채널공격(Side-channel attack) 기법인 전력분석공격(Power analysis attack)을 SRAM 기반 FPGA에 수행하여, FPGA가 재구성 될 때마다 내부의 복호화 회로가 동작하면서 발생하는 누설전력(leakage power)을 획득하고, 이것을 분석함으로써, 복호화용 키 저장공간에 저장된 복호화 키 정보를 획득 하는데 성공한 사례가 발표되고 있다.

4.3 비트스트림 인증

암호화된 비트스트림 데이터는 무결성(Integrity) 인증 기능은 제공하지 못하는 한계를 가진다. 즉, 공격자가 해당 FPGA의 서비스 무력화 (DOS Attack) 등을 목적으로 암호화된 비트스트림 파일의 내용을 임의로 변조하는 탬퍼링 공격(Tampering attack) 시도 시, FPGA 내부의 복호화 로직 회로는 공격자에 의해 변조된 비트스트림을 복호화하여 로직 설정 메모리(RAM)로 전달하므로, FPGA에는 비 정상적으로 변조된 디자인이 프로그래밍될 수 있다.

Xilinx는 2001년 Virtex-2에 디자인의 의도된 데이터 위/변조 방지를 위해 상용 FPGA로는 최초로 비트스트림 파일 자체에 3중 DES(triple DES) 암호화 및 무결성 인증 기술을 적용 하였다. 사실 간단히 생각해보자면, 보안적인 관점에서 위/변조 방지에 대한 방어는 암호화를 통해 기밀성을 유지한다기 보다는 무결성 인증기술 만이 필요하다고 생각할 수 있다. 하지만, 비트스트림 파일을 역공학하여 디자인 기능을 완벽히 복원할 수 있는 공격자 측면에서 생각해 보면, 암호화 하지 않을 경우 문제가 발생 할 수 있다. 즉 비트스트림 파일 부분에서는 메시지를 인증하는 부분만 삭제한 후에 비트스트림 파일을 재 컴파일 한 후 PROM 업로드하고, FPGA 내부의 무결성 인증부분에서는 비트플립 공격(Bit-flipping Attack)을 이용하여 메시지 인증 부분을 통과 시키는 방식으로 공격될 수 있다. 따라서, 암호화 기술의 적용은 필수적이라고 할 수 있겠다.

또한, 무결성을 보장하는 방법은, 수신한 비트스트림에 대한 위변조 여부를 확인 할 수 있겠지만, 그 메시지가 누구로부터 전송되는 것인지 확인 할 수 없다. 따라서 메시지 인증 절차가 없다면, 공격자가 정당한 사용자로 위장하여 메시지를 전송하는 위장공격이 가능해진다. 따라서 메시지 인증을 하기 위하여 메시지 인증코드(MAC)를 생성하여 메시지와 함께 전송하는 방법이 인증의 일반적인 방법이다.

최근 Altera 및 Xilinx 사에서 출시되는 SRAM 기반의 FPGA(Xilinx의 Virtex, Artix, Kintex 6 or 7 및 Altera Starix III)의 경우 무결성과 기밀성 보장을 위해 비트스트림 파일에 대한 인증과 256bit AES 암호알고리즘을 함께 이용하고 있는 추세이다.

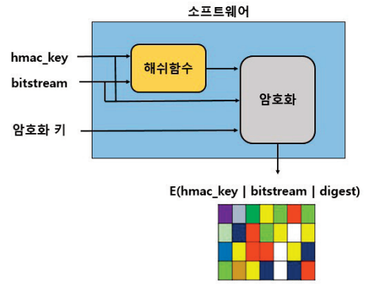


그림 8. Xilinx Virtex7의 소프트웨어 Hash생성과 암호화 과정

일반적으로 무결성 보장을 위한 인증은 SHA-256 해쉬 암호를 사용하는 HMAC (key-hashed message authentication code) 방법을 사용하며, 암호화는 AES-256 암호알고리즘을 이용하여 메시지 암호화를 수행한다. 그림 8은 Virtex 7의 소프트웨어 비트스트림 암호화와 해쉬 메세지 생성 과정을 보여준다. 이와 같은 방식은 소프트웨어를 이용하여 비트스트림 자체를 만들 때 메시지 인증 절차와 암호화가 같이 수행된 비트스트림 파일을 FPGA에 보내고, 그림 9의 수신 쪽인 FPGA는 사용자가 일전에 FPGA 내부에 탑재한 복호화키를 이용하여 복호화하고 메시지 인증 절차를 수행하면서, 메시지 자체에 대한 기밀성, 무결성, 인증을 통한 복제 방지 등을 모두 수행할 수 있게 구성되어 있다.

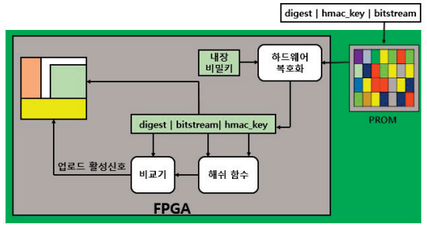


그림 9. FPGA에서의 복호화와 해쉬체크기

4.4 물리적복제방지

초기 FPGA 제품들은 작은 로직들만 구성이 가능한 프로토타입 형태의 디자인 용도로 출시 되었기 때문에 보안 기능들은 구성되어 있지 않았으며, FPGA 제조사들은 비트스트림 파일 생성에 대한 자세한 정보를 공개하지 않는 방식으로만 복제 방지를 유지하려고 노력하였다.

이후 FPGA 초기 복제 방지를 위한 방안으로 비트스트림 파일을 공격이 힘든 FPGA 내부 공간(안티퓨즈, 플래시)에 적재하여 사용함으로써 외부로 노출되는 것을 막는 방식만이 사용되었다. 하지만, 이러한 방식이 암호화를 따로 하지 않더라도 비트스트림 파일의 노출을 방지하기 때문에 보안적 관점에서 안전할 수는 있지만 상대적으로 큰 비트스트림 데이터를 유지하기 위해 전원을 계속 인가 시켜줘야 하는 것 같은 전력소모가 큰 단점이 있어 최근에는 사용되지 않고 있다.

Guajardo 등은 디자인의 복제방지 기법을 PUF(Physically Unclonable Function)을 적용하여 해결하고자 하였다. PUF는 반도체 제작 과정에서의 공정변이를 이용해 고유의 디바이스 DNA를 생성하기 때문에 이를 내장하여 FPGA를 설계할 경우 복제자체를 불가능하게 만든다.

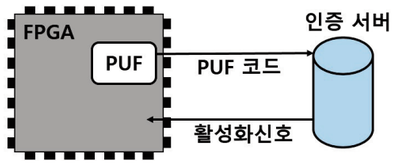


그림 10. PUF기반 인증 구조

Guajardo 등의 PUF 기반의 IP Protection 기법은 Intrinsic ID사의 Quiddikey-flex로 상용화 되었다. Quiddikey-flex는 등록부분과 인증부분으로 구분하고, 사용자의 FPGA에 내장되어 있는 PUF로부터 추출된 고유 값을 키로 사용하여, 생산단계에서 등록된 해당 고유 값을 서버로부터 인증 받아 사용을 허가 받는 시스템 권한을 받게 된다. 이렇게 PUF를 이용하여 서버로부터 고유 값을 인증 받아 동작되는 시스템의 경우 PUF 자체를 복제하는 것이 불가능하며, 동작코드 체크부분을 제거 불가능하기 때문에 공격자가 일반적인 방법으로는 소프트코어를 복제하지 못하게 만든다.

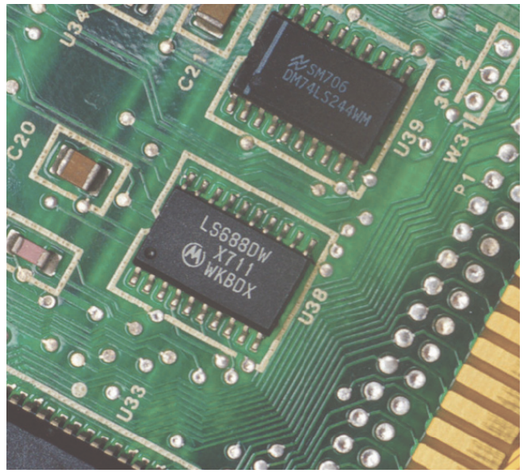
5. 결론

과거 FPGA가 단순히 시제품 제작을 위한 장치 위주로 사용되었으나, 최근에는 FPGA는 상용 시스템상에 주요 부품으로 사용되고 있는 추세에 따라 FPGA 자체에 대한 보안 이슈는 점점 더 많아 질 것으로 예상된다. 또한, 부채널 공격(side-channel attack) 기법인 전력 분석 공격을 FPGA에 적용하여 비트스트림 암호화키를 알아내는 공격 방식, 오류주입 공격을 통한 FPGA 비트스트림 인증절차의 무력화 등의 새로운 공격 방식이 소개됨에 따라, FPGA 보안에 대한 관심과 이슈가 더욱 많아질 것으로 생각되고, 해당 연구분야도 많이 활성화 될 것으로 생각된다.

홍 석 희 교수
소속 : 고려대학교 정보보호대학원(CIST)
연구분야 : Symmetric KeyPrimitives(Block/Stream Cipher, Hash Function), Asymmetric Key Primitives(Finite Field, ECC, Pairing), S/W & H/W implementation of Cryptographic Algorithms, Side-Channel Attack, Smart Grid Security
Email: shhong@korea.ac.kr
홈페이지: http://crypto.korea.ac.kr

김 현 민 박사과정
소속 : 고려대학교 정보보호대학원(CIST)
연구분야 : Asymmetric Key Primitives, Side-Channel Attack, Secure Logic Design, Asic & FPGA Design, S/W & H/W implementation of Cryptographic Algorithms, PUFs, Physical Level Security,Secure SOC design
Email: willguts@korea.ac.kr
홈페이지: http://crypto.korea.ac.kr

이 승 준 박사과정
소속 : 고려대학교 정보보호대학원(CIST)
연구분야 : ASIC & FPGA Design, S/W & H/W Implemenation of Crytographic, FPGA Security, Side-Channel Countermeasures for FPGA, FPGA Architecture, Secure Logic Design
Email: seungjoonlee@korea.ac.kr
홈페이지: http://crypto.korea.ac.kr



REFERENCE

[1]S. Drimer, ‘ ‘Security for volatile FPGAs,’ ’ Ph.D. dissertation, Comput. Sci. Dept.,Cambridge Univ., Cambridge, U.K., 2009

[2]ALTERA,” Anti-Tamper Capabilities in FPGA Designs” , Appl. Note, July. 2008.

[3]I.Hadzic, S.Udani, M. Smith, “FPGA viruses” , Field Programmable Logic and Applications 1999, pp 291-300

[4]Xilinx, E. Peterson, ‘ ‘Developing tamper resistant-designs with Xilinx Virtex-6 and 7 seriesFPGAs,’ ’ Appl. Note XAPP1084, 2012.

[5]Altera, ‘ ‘Using the design security features in Altera FPGAs,’ ’ Appl. Note, AN-556, Jun. 19,2013.

[6]A. Moradi, D. Oswald, C. Paar, and P. Swierczynski, “Side-channel Attacks on the Bitstream Encryption Mechanism of Altera Stratix II:Facilitating Black-box Analysis Using Software Reverse-engineering,” in Proc. the ACM/SIGDA International Symposium on FieldProgrammable Gate Arrays, ser. FPGA ’ 13, New York, NY, USA, 2013,pp. 91-100.

[7] Altera, “Stratix III design handbook” , Appl. Note, July .2010

[8] Xilinx, “7 Series FPGAs Configuration User Guide (UG470)” Appl. Note, June .2011

[9]J. Guajardo, S. S. Kumar, G. J. Schrijen, and

P. Tuyls, ‘ ‘Brand and IP protection withphysical unclonable functions,’ ’ in Proc. IEEEInt. Symp. Circuits Syst., 2008, pp. 3186-3189.

[10] Intrinsic-ID, ‘ ‘Quiddikey-Flex,’ ’ 2013. [Online]https://www.intrinsic-id.com/wp content/uploads/2014/10/Quiddikey-flex.pdf

[11]Xilinx, “CoolRunner-II CPLDs in SecureApplications” , Appl. Note, July .2002

Mentor 사 FloTHERM

Mentor사 FloTHERM

A. 목적

Thermal Analysis Solution

B. 구분

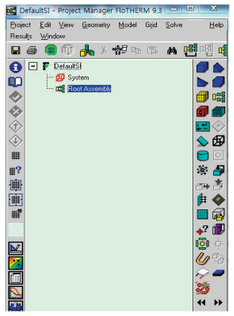
반도체부터 PCB, 시스템까지 모든 전자장비 내부와 주변의 공기 유동 및 열전달 예측

C. Supported Platform and O/S System

- Windows XP Professional 32/64bit
- Windows Server 2003 & 2003 R2 (Standard and Enterprise) 32/64bit
- Windows Server 2008 & 2008 R2 (Standard andEnterprise) 32/64bit
- Windows Vista (Business, Enterprise and Ultimate) 32/64bit
- Windows 7 (Professional, Enterprise and Ultimate)32/64bit
- Red Hat Enterprise Linux 4 and 5 (부분 지원) 32/64bit

D. 특성 및 기능

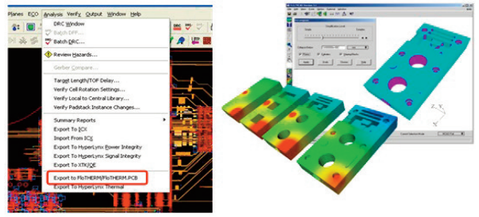
FloTHERM에서는 PCB에 실장된 단위 IC부터 많은 Board를 탑재한 Rack까지 전세계의 다양한 제조사가 제공하는 SmartParts (지능형 모델 생성 Macro)를 이용하여 손쉽게 모델을 구성할 수 있다.SmartParts를 활용함으로써 모델링 시간을 단축하고 결과의 정확성은 높일 수 있다.



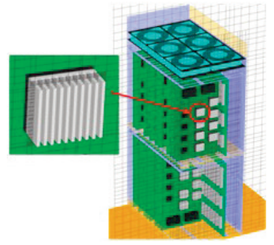
PCB, Fan, Heat Sink, Heat, Die, Heat Pipe, TEC, Compact Component 등 전자장비에서 자주 사용되는 요소들을 한 번의 클릭으로 쉽게 생성 가능한 SmartParts 제공

예를 들어 Thermo Electric Cooler (TEC) SmartPart를 사용해서 사용자가 특정 부품의 온도가 미리 지정해 놓은 온도 이상으로 높아지지 않도록 조절이 가능하다.또한, Fan RPM Derating 기능을 사용해서 목표 온도 이내에서 운용할 수 있는 최적 설계를 하는 것이 가능하다.

FloTHERM은 EDA 및 MCAD Tool 들과의 협업을 위한 솔루션도 제공하고 있다.FloMCAD Bridge를 사용하여 Pro/ENGINEER, SolidWorks, CATIA 등의 Native Data를 비롯하여 다양한 중립 포맷의 MCAD Data를 불러오는 것이 가능하다.BoardStation, Expedition PCB, Allegro, CR5000 등의 EDA tool들과의 직접 양방향 호환이 가능하여 PCBLay-out, 각 Layer Trace 정보, Via, Pad, Component 정보들을 손쉽게 적용할 수 있다. IDF Format 역시 지원하므로 폭넓게 EDA Tool들과 Data를 주고받을 수 있다.



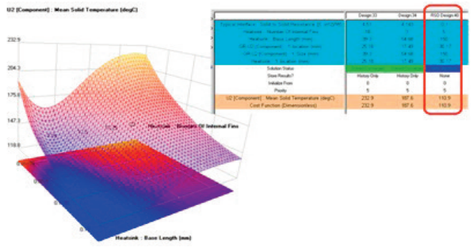
FloTHERM의 Grid는 가장 안정적이고 효율적인 Structured-Cartesian Method에 기반을 두고있다. Localized Grid를 이용하여 필요한 곳에는 더 많은 Grid를 사용하면서도 계산시간을 단축시키고 전체적인 Mesh 품질을 향상시킬 수 있다.FloTHERM의 Grid는 SmartPart와 연결되어 있으며 모델의 한 부분처럼 동작한다. 이 직관적인 Grid 방법은 사용자로 하여금 해석 그 자체보다는 설계에 더욱 집중할 수 있도록 해 준다.



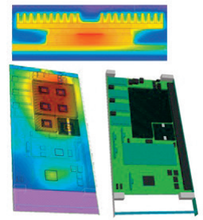
Mesh 작업에 많은 시간과 경험이 필요한 다른 Tool들과 비교해 FloTHERM의 Grid 작업은 즉각적이고 쉽다.

FloTHERM은 모델이 변경될 때마다 다시 Grid를 할 필요가 없는 유일한 해석 Tool이다.

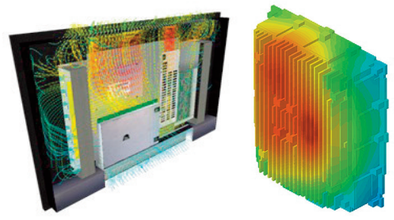
FloTHERM만이 가진 고유한 "Automatic Sequential Optimization"은 SmartPart 기반의 모델과 Structured Cartesian Grid의 조합으로 인하여 가능한 최적화 기능이다. 사용자가 설계 목표를 지정하면 FloTHERM은 그 목표를 만족시키기 위한 설계 변수의 최적 조합을 찾는 작업을 수행한다. Heat Sink 설계 최적화, PCB 부품 배치, Fan/Blower 선정과 같은 작업들은 손쉽게 수행할 수 있다.



20년 이상 FloTHERMSolver는 전자 냉각 분야에 특화되어 개발됐다. Localized Grid, Multi Grid 등의 테크닉을 이용하여 가장 빠른 시간내에 정확한 결과를 도출해낸다.



FloTHERM의 Post Processor는 해석 결과를 분석하는 작업의 효율성을 최대화시켜 준다.랜더링 모델, 3D Flow Animation, 온도 및 유동장에 대한 동적 계량 등의 기능을 이용하여 문제가 되는 부분이나 설계 효과를 쉽고 빠르게 시각화하여 확인할 수 있다. Texture Mapping이나 동영상 저장 등의 기능으로 기술자가 아닌 동료와의 협의도 가능하다. 최근에는 Bottleneck (Bn), Shortcut (Sc) 지수를 개발하여 현 설계에서의 열적 문제점 및 대책을 가시화하였다.



FloTHERM을 사용할 수 없는 환경에서는 별도로 제공되는 모든 기능을 포함한 Post-Processor인 FloVIZ를 이용하여 결과를 공유하는 작업에 이용할 수 있다.

회 사 명 : Mentor Graphics
웹 주 소 : http://www.mentorkr.com/
한국지사 : 한국멘토
전 화 : 031) 8061-0790
주 소 : 경기도 성남시 분당구 판교역로 192번길 12 (삼평동) 판교 미래에셋센터 7층

차세대 VLSI를 위한 광전자 집적회로 기술 (2)

플랫폼 기술

3회에 걸친 차세대 VLSI를 위한 광전자 집적회로 기술에 관한 내용 중 지난 첫 회에서는 반도체 기술의 발전 및 금속 배선 기술의 한계와 차세대 배선 기술로서의 광학 배선에 대해 소개하였다. 이후의 기고들에서는 광학 배선을 구현할 수 있는 기반 물질 및 요소 기술들에 관한 내용을 다루고자 한다.

1. 광학 배선에 있어서의 실리콘 기술의 난점

실리콘은 현대 전자공학의 핵심적인 기반 물질이며 다양한 종류의 전자 소자들의 개발이 실리콘을 기반으로 하여 이루어지고 있다. 실리콘 전자 소자들의 성능을 향상시키기 위해 일부 기능성 물질들을 국부적으로 도입하는 연구들도 활발히 이루어지고 있으나 경제성과 오랜 시간에 걸쳐 축적된 안정적인 공정 기술로 인해 적어도 실리콘 기판을 유지하는 기술 구현을 추구하고 있다. 근래 CMOS 호환성(CMOS compatibility)라는 표현을 자주 접하게 되는데 CMOS는 적절한 공정만 뒷받침된다면 어떠한 반도체에서도 구현할 수 있고 그간의 CMOS 기술은 거의 대부분 실리콘을 기반으로 이루어져 왔다는 점을 상기해볼 때, 그러한 표현들이 전하고자 하는 보다 정확한 의미는 실리콘 호환성(silicon compatibility)이라고 이해하는 것이 옳을 것이다.

이러한 관점에서 볼 때, 광학 배선은 기존의 실리콘 기반의 CMOS 집적회로에 접목하려는 노력부터 시작되었을 것임은 의심의 여지가 없다. 광학 배선은 배선으로서의 광도파로(optical waveguide) 자체 뿐만 아니라, 광 검출기(photodetector), 광 변조기(optical modulator), LED(light-emitting diode)와 레이저 등의 광원을 포괄한다. 여타의 요소들은 실리콘을 기반으로 하여 구현이 가능하지만 대표적인 간접 밴드갭 물질로서 발광 효율이 매우 낮은 실리콘으로 광원을 구현하는 것은 어려운 일이다. 실리콘에서의 발광을 위한 연구들이 이미 적극적으로 이루어져 왔으나, 발광 효율 자체를 높이는 데에는 어느 정도 성공한 사례들이 있다 하더라도 여전히 실용적인 수준에서의 발전이 이루어졌다고 보기에는 어려움이 많으며 아직은 실리콘 기반의 집적회로와의 공정 호환성보다는 가능성 자체를 보려는 시도인 경우들이 많다[1,2].

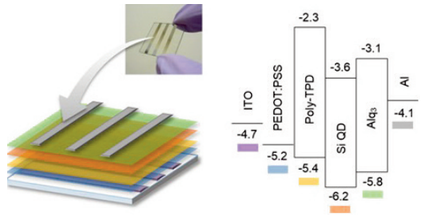


그림 1. 실리콘 양자점을 활용한 실리콘-유기물 기반의 백색광 LED[2].

2. 실리콘 기반의 광원 구현을 위한 이종접합 기술: 본딩 기법 (chemical mechanical bonding)

실리콘 기판에서 광원을 구현하기 위한 방법으로서는 서로 다른 기판의 물리적인 본딩(bonding)이 오래 전부터 시도되어 왔으며 이미 상용화에 성공한 기술이다(그림 2). 즉, 신호 처리를 위한 CMOS 회로 영역은 실리콘으로 구현을 하고 광원은 III-V 화합물 반도체로 제작하여 서로 물리적으로 결합하는 방식이다. 이 때, 공정과 본딩의 순서는 서로 바뀔 수 있으며 직접 밴드갭 물질 여부가 크게 중요하지 않은 수동 광학 소자들은 실리콘이나 III-V 화합물 반도체 영역 모두에서 제작될 수 있으므로 공정 집적(process integration)과 성능 지표를 고려하여 둘 중 한 플랫폼을 결정하거나 양쪽 모두에 복합적으로 구현할 수 있다(그림 3).

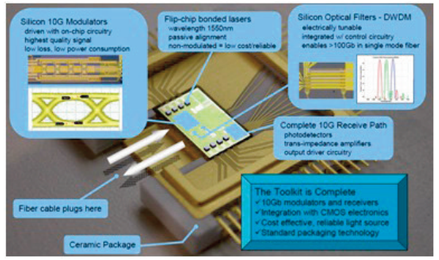


그림 2. 실리콘 기반의 CMOS 회로, 실리콘 광학 변조기, 실리콘 광학 필터를 집적한 회로에 본딩 기술을 통해 레이저 회로를 결합한 광전자집적회로. 이 집적회로를 상용화한 Luxtera 社는 이 기술을 통해 CMOS Photonics라는 트레이드마크를 보유하고 있다.

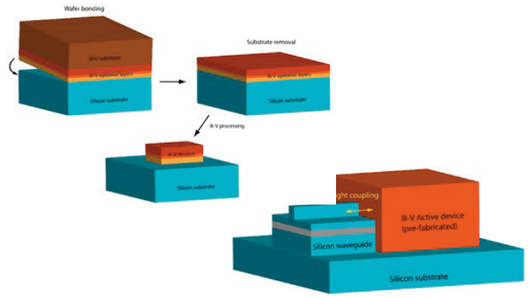
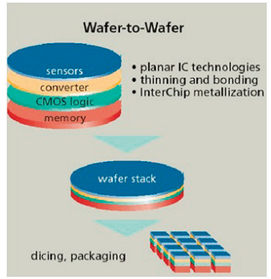
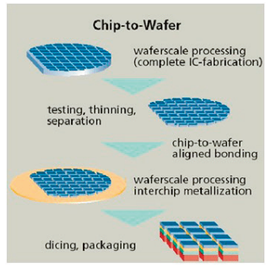


그림 3. 웨이퍼본딩 후 소자 제작을 통한 이종집적 기술. III-V 화합물 반도체 기판 또는 결정 정합성을 갖는 기판 상에 III-V 화합물 반도체의 에피택시 → 고온, 고압 상태에서의 실리콘 기판과의 본딩 → 각 영역에서의 소자 제작.

본딩 기술은 다음의 그림 4(a)와 4(b)에서 볼 수 있는 바와 같이, 좀 더 세부적으로는 웨이퍼 투 웨이퍼(wafer-to-wafer) 본딩과 칩 투 웨이퍼(chip-to-wafer) 본딩 기술로 구분할 수 있다.



(a)



(b)

그림 4. 두 가지 접근을 통한 본딩 기술. (a) 웨이퍼 투 웨이퍼 및 (b) 칩 투 웨이퍼 본딩 기술.

웨이퍼 간 본딩을 수행할 때에 하부 웨이퍼에서의 회로 제작을 진행하고 상부 웨이퍼를본딩한 후 습식식각을 통해 1~2 μm 수준으로 얇게 만들면(thinning) 충분한 수준의 투명도를 얻게 되어 사진 공정(photolithography) 시 하부 웨이퍼의 회로들에 정렬(align)하여 이후 상부 웨이퍼에서의 공정을 수행할 수 있다. 상하부 회로 간 수직적인 형태의 배선이 가능하며 상부 웨이퍼의 두께가 얇아 컨택 홀(contact hole)의 크기도 충분히 작게 형성할 수 있어 집적회로가 차지하는 면적을 줄일 수 있는 효과도 기대할 수 있다. 이 기술의 단점은 전체 공정 비용이나 집적회로의 수율이 상부 웨이퍼의 크기에 의해 결정된다는 점이다. 즉, 실리콘 기판에 InP나 GaAs 등의 III-V 화합물 반도체 기판을 본딩하게 되는데 근래 통용되는 실리콘 기판과 같은 수준의 크기로 이들 화합물 반도체 기판을 제작하는 것은 매우 높은 비용이 들게 된다.

4인치 미만의 화합물 반도체 기판을 주로 사용하게 되는데 이는 제작 가능한 칩의 전체 수가 하부 기판의 면적이 아닌 상부 기판의 면적에 의존하므로 경제성 측면에서 매우 유리한 기술이라고 보기에는 어려움이 있다. 칩 투 웨이퍼 본딩은 본딩하고자 하는 기판 상에서 회로 제작을 완료한 후 다이(die)별로 다이싱(dicing)을 하여 모체가 될 웨이퍼에 개별적으로 본딩하는 기술이다. 하부의 회로와 수평적인 배선이 이루어져야 하므로 집적도 측면에서는 다소 불리할 수 있으나 웨이퍼 간 본딩 기술에서와 같이 박막화를 한 후 본딩함으로써 어느 정도 그러한 문제를 해결할 수 있다. 마스킹 처리가 선행되기는 하지만 상부 웨이퍼에서의 공정 동안 진행되는 열 및 화학적 공정들을 이미 제작된 하부 웨이퍼의 집적회로가 같이 거쳐야 한다는 문제점을 제거할 수 있다는 장점이 있는 반면, 집적회로의 초소형화와 본딩 과정 자체에서의 수율 문제 등은 개선의 여지가 있다.

3. 실리콘 기반의 광원 구현을 위한 이종접합 기술: 격자 상수 조절(bandgap engineering)

실리콘에 게르마늄(germanium)을 넣게 되면 전자 및 정공 이동도가 향상되는 현상이 잘 알려져 있다. 1990년대 중반 이후 활발히 연구되어 온 SiGe 기술은 SiGe을 채널 물질 뿐만 아니라 접합 물질에 적용하여 채널에 대한 압축을 가하기 위한 용도(stressor)로 사용되고 있다. 순수한 게르마늄은 운동량 공간에서 전도대 최솟값의 위치가 가전자대 최댓값의 위치와 서로 어긋나 있어 구분상으로는 실리콘과 더불어 대표적인 간접 밴드갭 물질이다. 그러나 감마 밸리(k = 0)에서 전도대의 E-k 다이어그램이 극소값을 갖는 독특한 전자 구조로 인해, 적절한 방식으로 그곳에 전자들을 충분히 분포시킬 수 있다면 발광 효과를 얻을 수 있다. 나아가, 그림 5에서 보는 바와 같이 게르마늄에 인장력을 가하게 되면 캐리어 이동도가 증가함과 동시에 감마 밸리의 극소값이 더욱 작아지고 직접 밴드갭 물질로 바뀌는 효과까지 기대할 수가 있다[3]. 실리콘 포토닉스는 모든 것을 실리콘에서 구현하는 것만을 의미하는 것이 아니라 실리콘과 집적성이 좋은 물질에서의 포토닉스를 포함하므로[4], 실리콘과 합금(alloy)를 형성하기 용이한 게르마늄에서 광원을 구현할 수 있다면 실리콘 광학에서의 성공이라고 간주해도 큰 무리가 아닐 것이다.

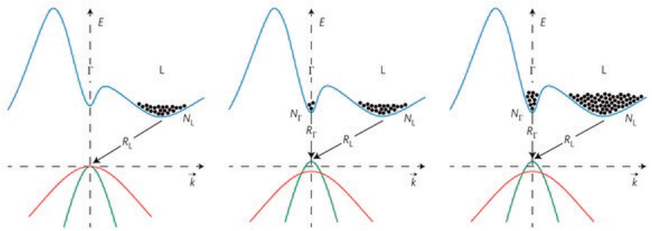


그림 5. 인장력이 증가함에 따른 게르마늄의 에너지 밴드 구조의 변화[5]. 직접 밴드갭 물질로 변화하면서 감마 밸리에서의 전자 분포 확률이 크게 증가하게 된다.

위와 같이 게르마늄에 인장력을 가하는 방법에는 크게 두 가지 방법이 제시되고 있는데 열팽창 계수가 다른 물질을 압축기로 사용하는 방법과 게르마늄보다 원자 반경이 큰 원소를 넣어 격자 상수를 키우는 방법이다. 전자의 접근을 위해서 게르마늄 영역을 박막화한 후 압축을 가하게 되면 더욱 큰 효과를 기대할 수가 있다. 후자의 방법은 보다 근래 시도되고 있는 방법으로 그에 사용하는 원소로서 실리콘, 게르마늄과 같은 4족이면서 게르마늄 바로 다음 주기에 있는 Sn(stannum, 주석, tin)를 들 수 있다[5]. 게르마늄이 실리콘에 대해서 하던 역할을 주석이 게르마늄에 대해서 해줄 것으로 기대할 수 있는 것이다.

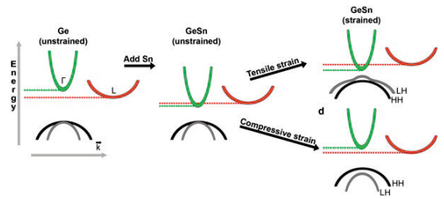


그림 6. 주석의 주입에 따른 게르마늄의 에너지 밴드 구조의 변화[6].

그림 6은 주석을 주입함에 따라 게르마늄의 에너지 밴드 구조가 어떻게 변화하는지를 모식적으로 나타낸다[6]. 앞서 살펴본 그림 5에서 인장력을 가할 때의 결과와 유사한 변화 경향성을 보여준다. 아무런 외력이 가해지지 않은 게르마늄을 직접 밴드갭 물질로 바꾸는 데 필요한 주석의 함량은 약 7%이나 압축력이 가해진 상태에서의 게르마늄을 바꾸기 위해서는 최소 10% 이상의 함량이 필요하다. 그림 6에서 보는 바와 같이 압축력은 게르마늄의 감마 밸리 극소값을 다시 위로 올리는 효과를 주기 때문인데, 게르마늄보다 격자 상수가 작은 실리콘은 게르마늄에 대하여 압축력을 가하므로 실리콘 기반의 게르마늄 및 게르마늄 틴 기술을 적용한 광전자 집적회로 구현을 위해서는 주석의 함량을 충분히 높여주어야 하며 이를 위한 공정 개발 연구가 다각적으로 이루어지고 있다. 이론적인 계산과 광여기 발광(photoluminescence) 등의 기초 실험 외에도 실제 GeSn을 기반으로 한 광학 공진기 제작과 성능 분석을 통해 주석을 함유한 게르마늄의 밴드갭이 작아져 공진이 발생하기 시작하는 광신호의 파장이 순수한 게르마늄의 감마 밸리 에너지에 해당하는 파장인 1.55 μm 보다 긴 영역에서 측정되는 결과가 보고되기도 하여[7], 게르마늄 틴 역시 실리콘 기반의 광원 소자를 구현할 수 있는 플랫폼으로서 기능할 수 있는 가능성이 크다.

4. 맺음말

실리콘 기반에서 CMOS 회로와 집적 가능한 광학 배선을 구현할 수 있도록 하는 플랫폼 기술에 대하여 살펴보았다. 물리적 • 화학적 방법을 통해 직접적으로 본딩하는 기술과 격자 상수 변화를 통해 기반 물질 자체의 광학적 특성을 향상시키는 접근 기술 두 가지를 들 수 있다. 전자는 기술이 많은 부분 성숙했지만 비용과 수율 측면에서의 개선의 여지를 남겨두고 있으며 후자는 소자 및 회로의 집적공정 수행 과정 자체에서 접근할 수 있는 방법이나 본딩에 비해 가시적인 효과가 상대적으로 작고 아직 공정 개발이 더욱 심도 있게 이루어져야 하는 단계에 있다. 이처럼 각 플랫폼 기술에는 장점과 단점이 엄연히 존재하지만 실리콘 기반의 광집적회로 및 광학 배선 기술은 더 이상 미래의 기술이 아니라 이러한 플랫폼 기술들을 통해 이미 실현 가능한 활로가 충분히 마련되었다는 희망을 가질 수 있다. 다음의 마지막 연재에서는 동일한 플랫폼에서의 광학 배선을 구성할 수 있는 전자 소자 및 광학 소자들과 관련 연구 개발 현황을 살펴보고자 한다.

조 성 재 교수
소속 : 가천대학교 전자공학과
주 연구분야 : 나노전자소자 및 광학소자
E-mail : felixcho@gachon.ac.kr

참고문헌

[1] W. L. Ng, M. A. Lourenco, R. M. Gwilliam, S. Ledain, G. Shao, and K. P. Homewood, "An efficient room-temperature silicon-based light-emitting diode," Nature, vol. 410, no. 6825, pp. 192-194, Mar. 2001.

[2] Y. Xin, K. Nishio, and K. Saitow, "White-blue electroluminescence from a Si quantum dot hybrid light-emitting diode," Applied Physics Letters, vol. 106, no. 20, pp. 201102-1-201102-5, May 2015.

[3] J. R. Jain, A. Hryciw, T. M. Baer, D. A. B. Miller, M. L. Brongersma, and R. T. Howe, "A micromachining-based technology for enhancing germanium light emission via tensile strain," Nature Photonics, vol. 6, no. 6, pp. 398-405, May 2012.

[4] G. T. Reed and A. P. Knights, Silicon Photonics, John Wiley & Sons, New Jersey, USA, 2004,

[5] J. S. Harris, H. Lin, R. Chen, Y. Huo, E. Fei, S. Paik, S. Cho, and T. Kamins, "MBE Growth of GeSn and SiGeSn Heterojunctions for Photonic Devices," ECS Transactions, vol. 50, no. 9, pp. 601-605, Oct. 2012.

[6] R. Chen, S. Gupta, Y.-C. Huang, Y. Huo, C. W. Rudy, E. Sanchez, Y. Kim, T. I. Kamins, K.C. Saraswat, and J. S. Harris, "Demonstration of a Ge/GeSn/Ge Quantum-Well Microdisk Resonator on Silicon: Enabling High-Quality Ge(Sn) Materials for Micro- and Nanophotonics," Nano Letters, vol. 14, no. 1, pp. 37-43, Jan. 2014.

[7] S. Cho, R. Chen, S. Koo, G. Shambat, H. Lin, N. Park, J. Vučković, T. I. Kamins, B.-G. Park, and J. S. Harris, Jr., "Fabrication and Analysis of Epitaxially Grown $Ge_{1-x}Sn_x$ Microdisk Resonator with 20-nm Free-Spectral Range," IEEE Photonics Technology Letters, vol. 23, no. 20, pp. 1535-1537, Oct. 2011.