반도체설계교육센터
IC DESIGN EDUCATION CENTER

IDEC Newsletter

IDEC Newsletter | 통권 : 제19[illegible]호 | 발행일 | 2013년 10월 31일 | 발행인 | 박인철 | 편집인 | [illegible] | 제작 | 주을디자인
[illegible] | 042) 35[illegible]535 팩 스 | 042) 350-8[illegible] 홈페이지 | http://[illegible]
E-mail | [illegible]@idec.or.kr 발행처 | 반도체설계교육센터(IDEC)

Vol.197

2013
November

반도체설계교육센터 사업은 산업통상자원부, 한국반도체산업협회, 반도체회사(삼성전자, SK하이닉스, 매그나칩반도체, 동부하이텍, 앰코테크놀로지코리아, KEC, 세미텍, TowerJazz)의 지원으로 수행되고 있습니다.

멀티 코어 멀티 태스크 시스템의 최악 성능 예측 기술

MPSoC를 설계하면서 시스템 수준에서 최악 성능을 예측하는 것은 실시간 제약 조건을 갖는 시스템의 설계에 반드시 필요한 작업이다. 경성 실시간 응용의 경우 데드라인을 만족시키는 못하면 치명적인 결과를 유발하기 때문에 어떤 경우에도 데드라인을 만족시키도록 시스템을 설계하여야 한다. 최악 성능을 과도하게 예측을 하게 되고 그 예측에 기반을 두어 시스템을 설계하게 되면, 시스템의 제작비용이 많이 증가하는 단점이 생긴다. 이뿐 아니라 주어진 응용을 수행하는데 필요한 성능 이상을 제공하는 프로세서를 사용하게 되면 전력 소모도 많아지고 열도 많이 발생하게 된다. 아울러 시스템의 안전도에도 영향을 미치게 될 것이다. 본 고에서는 멀티 코어 멀티 태스크 시스템의 최악 성능 예측 기술에 대해 알아보고자 한다. (관련기사 P04~7참조)

전자파 및 전력 소모량 측정 등 다양한 부채널 분석을 통한 암호모듈 분석 소개

스마트카드나 RFID 같은 소형 전자 장비의 사용이 늘어나면서 이러한 장비들에 대한 물리적인 보안 문제가 중요한 이슈로 떠오르고 있다. 특히, 부채널 분석을 이용한 방법은 칩에 손상을 입히지 않고 칩 안에 저장된 비밀정보를 얻어내는 공격방법이기 때문에 관련 공격에 대한 대응책이 고려되어야 한다. 즉, 스마트카드의 활용분야가 확대되면서 IC 칩의 물리적인 안전성에 대한 관심이 높아지고 있다. 본 고에서는 스마트카드에 많이 사용되는 타원곡선 암호 알고리즘에 대한 전력 분석 공격 및 전자파 분석 공격의 최신동향에 대해 알아보고 이러한 공격을 통해 알고리즘의 안전성을 분석 및 평가하는 방법에 대해 설명하고자 한다. (관련기사 P08~13참조)

Prime 2013 참가후기 및 기술 트렌드

Prime 2013은 2013년 6월 24일부터 27일까지 오스트리아 빌라흐에서 개최되었다. 정상 수준의 산업계와 학계 연구진들이 기술위원으로 위촉되었고 연구 트렌드와 발전방향에 관한 훌륭한 초청강연들도 준비되어 있었다. DC와 RF뿐만 아니라 아날로그에서 디지털까지 전자공학의 거의 모든 분야 및 애플리케이션까지 망라하여 우수한 논문들이 많이 발표되었다. 본 본 고에서는 학회에 참석한 경북대 최준림 교수의 시선으로 Prime 2013의 Power Management 세션 및 Infinieon의 Plenary Paper에서 소개된 기술 및 동향을 참가 후기 형식으로 살펴보고자 한다. (관련기사 P14~16참조)

Aldec 사의 Active-HDL

Aldec 사의 Active-HDL 툴은 FPGA design과 시뮬레이션솔루션 관련 설계 플로우 관리자를 통합 제공한다. Active-HDL은 FPGA용 디자인 Simulator로서, VHDL, Verilog, SystemC 그리고 EDIF, C/C++와 SystemVerilog format을 지원한다. VHDL, Verilog, EDIF(netlist), 또는 Mixed-HDL(VHDL and Verilog and EDIF)을 Single Kernel에서 시뮬레이션할 수 있으며, Optimized Direct Compile Architecture를 사용함으로써 최고의 성능과 우수한 기능(디버깅 환경)을 갖는 고성능의 HDL Simulator이다. 본 고에서는 Aldec 사의 Active-HDL을 소개하고자 한다. (관련기사 P18~19참조)

IDEC news November | 2013

MPW (Multi-Project Wafer)

2013년 MPW 진행 현황

공정	MPW 회차	제작가능면적 (면적㎟x칩수) /회별	채택 팀수	설계면적 ((면적)x칩수)	DB마감	Die -out	비고
삼성 65nm (년3회)	119	(4x4㎟) x 48	23	(4x4)x23	13.03.15	13.08.15	★제작완료
	121		29	(4x4)x29	13.07.05	13.12.06	제작중
	126		37	(4x4)x37	13.11.08	14.04.11	설계중
MH 0.18um (년4회)	118	(4.5x4㎟) x 20	23	(4.5x4)x17 (4.5x2)x6	13.02.18	13.07.22	★제작완료
	120		20	(4.5x4)x20	13.05.06	13.10.04	★제작완료
	122		20	(4.5x4)x20	13.07.29	13.12.24	제작중
	125		24	(4.5x4)x16 (4.5x2)x8	13.10.21	14.03.25	DB 검토중
MH 0.35um (년2회)	121	(5x4㎟) x 20	20	(5x4)x20	13.06.17	13.10.04	PKG 제작중
	127		20	(5x4)x20	13.12.02	14.03.25	설계중
동부 0.11um (년2회)	119	(5x2.5㎟) x 24	27	(5x2.5)x20 (2.5x2.5)x7	13.03.20	13.07.31	★제작완료
	124		26	(5x2.5)x20 (2.5x2.5)x6	13.09.11	14.01.22	제작중
동부 0.18um BCD (년4회)	120	(5x2.5㎟) x 4	4	(5x2.5)x4	13.05.15	13.08.28	★제작완료
	121		4	(5x2.5)x4	13.06.26	13.10.09	★제작완료
	123		4	(5x2.5)x2 (2.5x2.5)x2	13.08.21	13.12.04	제작중
	126		5	(5x2.5)x3 (2.5x2.5)x2	13.11.13	14.02.06	설계중
동부 0.35um BCD (년4회)	118	(5x2.5㎟) x 6	6	(5x2.5)x6	13.02.27	13.06.12	★제작완료
	120		10	(5x2.5)x2 (2.5x2.5)x8	13.05.01	13.08.14	★제작완료
	123		6	(5x2.5)x6	13.08.14	13.11.27	제작중
	125		7	(5x2.5)x5 (2.5x2.5)x2	13.10.23	14.02.05	DB 검토중
TJ SiGe (년1회)	119	(2.5x2.5㎟) x 4	4	(2.5x2.5)x4	13.03.12	13.07.01	★제작완료
TJ CIS (년2회)	120	(2.5x2.5㎟) x 4	4	(2.5x2.5)x4	13.05.06	13.09.16	★제작완료
	125		4	(2.5x2.5)x4	13.10.14	14.02.17	DB 검토중
TJ BCD (년2회)	120	(5x2.5㎟) x 4	2	(5x5)x1 (5x2.5)x1	13.05.20	13.09.16	★제작완료
	125		2	(5x5)x2	13.10.21	14.02.17	DB 검토중
TJ RF (년2회)	120	(2.5x2.5㎟) x 4	4	(2.5x2.5)x4	13.05.20	13.09.16	★제작완료
	125		4	(2.5x2.5)x4	13.10.21	14.02.17	설계중

* 일정은 사정에 따라 다소 변경될 수 있습니다.
* 기준 : 2013. 10. 23

* 2014년 MPW 일정 및 모집 안내 : 11월 중 홈페이지를 통해 공지 예정

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

NDA가 체결된 Design Data 유출 금지 안내

IDEC의 MPW 참가를 통해 전달받은 Design Data 일체는 NDA를 통해서 법적인 구속력을 가지며, 관리 소홀로 인한 외부로의 공개 또는 유출 시 개인뿐만 아니라 개인이 속해 있는 WG에 자격 박탈과 같은 강력한 규제가 가해질 수 있습니다. 협약에 의해, 형사상 책임을 물을 수 있음을 알려 드립니다. MPW 참여자 분들은 Design Data 및 관련 자료의 관리를 철저히 하시어 불이익을 당하는 일이 없도록 거듭 당부 드립니다. NDA 체결 후 수령한 Design Kit 일체는 IDEC에 칩 수령 후 2개월 이내에 반드시 삭제하고, NDA 폐기확인서를 제출하여 제3자에 의한 공개 및 유출이 일어나지 않도록 주의 바랍니다.

2013년 11월 교육프로그램 안내

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

센터별 강좌 일정 |

센터명	강의일자	강의제목	분류
KAIST	11월 27일	무선전력전송용 송수신 회로 설계	설계강좌
부산대	11월 07일-08일	ICC tool을 사용한 P&R 교육	Tool강좌
	11월 22일-23일	USN/IoT 시스템의 기초와 응용	설계강좌

▷KAIST 개설 강좌 안내

■ 강좌일 : 11월 27일
■ 강좌 제목 : 무선전력전송용 송수신 회로 설계
■ 강사 : 이강윤 교수 (성균관대학교)

[강좌개요]
무선 전력 전송의 효율을 향상시키기 위한 시스템 구조 및 Rectifier, DC-DC Converter, LDO Regulator, Power Amp 등에 대해서 기본적인 동작 원리부터 최근 설계 동향에 대해서 다룬다.

[수강대상]
· 석박사 과정 대학원생, 산업체 연구원

[강의수준] [강의형태]
· 중급 · 이론

[사전지식,선수과목]
· 회로이론, 전자회로 1,2, 아날로그 집적회로

* 문의 : KAIST IDEC 구재희 (042-350-8536, kjh9@idec.or.kr)

■ 강좌일 : 11월 7일-8일
■ 강좌 제목 : ICC tool을 사용한 P&R 교육
■ 강사 : 손병복 연구소장/상무 ((주)이디에이엘리텍), 조현우 책임연구원/차장 ((주)이디에이엘리텍)

[강좌개요]
본 강좌에서는 실무에 적용 가능한 ICC tool의 활용 방법을 배우고 P&R설계에 필요한 DesignKit의 활용법과 배경 지식을 습득하고 이해하는 것을 목표로 한다.

[수강대상]
· 대학원생

[강의수준] [강의형태]
· 중급 P&R(Back-end) 강의 · 이론+실습

[사전지식,선수과목]
· Design Compiler, PrimeTime(STA), ICC 사용(교육) 경험이 있는 자

■ 강좌일 : 11월 22일-23일
■ 강좌 제목 : USN/IoT 시스템의 기초와 응용
■ 강사 : 유수봉 교수 (안양대학교), 박수은 수석연구원 (셀로코 전자기술연구소)

[강좌개요]
정보화 사회 및 인터넷 기술은 더욱더 우리사회 전반에 깊숙이 스며들고 있는데, 그 핵심기술이 USN 시스템 기술이고, 그 속에는 센서네트워크가 자리하고 있다. 근간에는 영상처리가 USN에서도 더욱 중요해지는데, 여기에 대한 해결책은 반도체 SOC를 필요로 한다. 본 강좌에서 USN SOC부터 센서네트워크, 영상 USN System 전체를 이해하고, 실제 영상 USN 시스템으로 실습 경험한다.

[수강대상]
· USN 시스템 관심자, 센서네트워크 개발자

[강의수준] [강의형태]
· 대학 2~3학년 , 초+중급 · 이론+실습

[사전지식,선수과목]
· 전자공학 기초, MCU 제어

* 문의 : 부산대 IDEC 윤성심, 지화준 (051-510-2828, idec@pusan.ac.kr)

Chip Design Contest (CDC)

■ International SoC Design Conference(ISOCC) 2013 Chip Design Contest 개최

1. 일정 및 장소

가. 일정 : 2013년 11월 18일(월)
나. 장소 : BEXCO Convention Hall, 부산

2. 행사 진행 일정

구분	시간	비고
데모/패널 전시	09:00 ~ 16:00	- 패널팀 전시 : 171팀(오전/오후로 나눠 전시) - 데모팀 전시 : 20팀
패널 발표	CDC-1 09:00 ~ 09:45	- 정규세션으로 편성됨 : 15개팀 발표(15분/팀) - 룸 별도 배정 됨(동일룸에서 진행)
	CDC-2 13:30 ~ 15:00	
	CDC-3 15:30 ~ 17:00	
시상식	17:30 ~ 19:30	- Banquet

* 일정은 사정에 따라 다소 변경될 수 있음.

3. 시상 내역

Award 명	수상팀수	내 역
Best Design Award	1팀	상장 및 상금 100만원
Best Demo Award	- 3개팀 - 특별상(SSCS 서울챕터상) 1팀	각 상장 및 상금 50만원
Best Poster Award	- 8개팀	각 상장 및 상금 20만원

■ 제21회 한국반도체학술대회(KCS) Chip Design Contest 개최

1. 일정 및 장소

가. 일정 : 2014년 2월 25일(화)
나. 장소 : 한양대학교, 서울

2. 논문 마감 : 2013년 11월 08일

- 논문 접수 분야 : SoC 설계

3. MPW 설계팀 참여 대상

- 2013년 MPW(118회~120회, 8월말까지 제작된 공정) + 2012년 MPW 미제출팀

4. 시상내역

Award 명	수상팀수	내 역
Best Design Award	1팀	상장 및 상금 100만원
Best Demo Award	- 2개팀 - 특별상(SSCS 서울챕터상) 1팀	각 상장 및 상금 50만원
Best Poster Award	- 5개팀 내외	각 상장 및 상금 20만원

* 수상팀 수는 참여팀 수 등에 따라 조정될 수 있음.

※ 관련 사항

* CDC 참여와 관련한 자세한 사항은 홈페이지(http://idec.or.kr)를 참조
* 담당 : 구재희 선임(042-350-8536, kjh9@idec.or.kr)

* 문의 : 구재희(042-350-8536, kjh9@idec.or.kr)

멀티 코어 멀티 태스크 시스템의 최악 성능 예측 기술

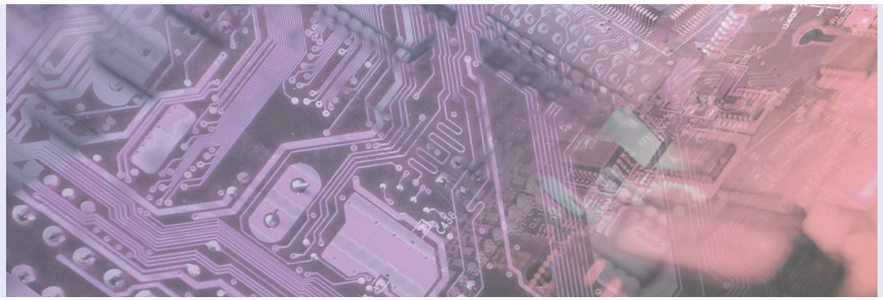
서울대학교 컴퓨터공학부

하순회 교수

연구분야 : 임베디드 시스템 설계방법론, 병렬임베디드 소프트웨어, HW/SW 통합설

E-mail : sha@iris.snu.ac.kr

http://peace.snu.ac.kr/sha/



MPSoC를 설계하면서 시스템 수준에서 최악 성능을 예측하는 것은 실시간 제약 조건을 갖는 시스템의 설계에 반드시 필요한 작업이다. 경성 실시간 응용의 경우 데드라인을 만족시키는 못하면 치명적인 결과를 유발하기 때문에 어떤 경우에도 데드라인을 만족시키도록 시스템을 설계하여야 한다. 따라서 문제는 얼마나 정확히 최악 성능을 예측할 수 있는가이다.

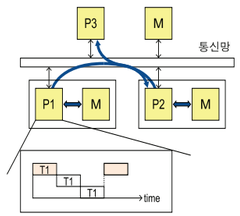
최악 성능을 과도하게 예측을 하게 되고 그 예측에 기반을 두어 시스템을 설계하게 되면, 시스템의 제작비용이 많이 증가하는 단점이 생긴다. 이뿐 아니라 주어진 응용을 수행하는데 필요한 성능 이상을 제공하는 프로세서를 사용하게 되면 전력 소모도 많아지고 열도 많이 발생하게 된다. 아울러 시스템의 안전도에도 영향을 미치게 될 것이다.

최악 성능 분석의 문제는 여러 수준에서 정의된다. 먼저 입력 조건에 따라 수행 시간이 변화하는 태스크에 대한 최악 수행시간 분석 문제는 코드를 기본 블록(Basic block)단위의 제어-데이터 플로우 그래프로 변환하고 최악 수행 경로를 찾는 것이 일반적인 해법이다. 상위 수준의 분석에서는 각 태스크의 수행시간 범위가 [BCET, WCET]의 구간으로 주어진다고 가정한다.

BCET는 Best-case execution time의 약자로 가장 짧은 수행시간을 의미하고 WCET는 worst-case execution time의 약자로 가장 긴 수행시간을 의미한다.

한 프로세서에 여러 태스크가 동시에 수행될 때에 다른 태스크들의 영향으로 어떤 주어진 태스크의 수행시간이 얼마나 길어질 수 있는지를 분석하는 컴포넌트 수준의 최악 수행시간 분석은 실시간 시스템 분야에서 오랫동안 연구되어온 문제이다. 태스크들의 CPU와 버스 등의 하드웨어 자원을 공유하기 때문에 발생하는 지연과 스케줄링 우선순위에 따라 지연되는 것을 모두 고려해야 한다.

아래 그림 1(a)에 3개의 태스크가 하나의 프로세서에서 실행될 때에의 스케줄을 하나 예시하였다. 그림에서 태스크 T1이 우선순위가 높은 태스크 T2와 T3에 의하여 선점되어 실행이 지연되는 것을 볼 수 있다.



(b) 시스템 수준 최악 성능 분석

(a) 컨포넌트 수준 최악 성능 분석

그림 1. 최악 성능 분석 문제의 수준별 구분

시스템 수준의 최악 성능 분석은 다수의 프로세싱 컴포넌트가 통신 네트워크로 연결된 병렬 시스템에서 여러 응용 프로그램들이 서로 간섭을 일으키며 수행되는 경우, 특정 응용 프로그램의 최악 수행 시간을 분석하는 문제이다.

그림 1의 (b)에는 프로세서 P1에 있는 태스크가 P2에 있는 태스크로 메시지를 전송하고 P2에 있는 태스크가 P3에 있는 태스크로 메시지를 전송하는 패턴이 굵은 화살표로 표시되어 있다.

이러한 태스크 간의 메시지 전송 경로를 통해서 응용이 수행된다고 할 때에 최악 성능을 구하기 위해서는 P1, P2, P3 각 프로세서 내부에서의 수행 시간과 통신망에서의 수행 시간을 모두 고려한 최악 성능을 구해야 한다.

즉, 시스템 수준의 최악 성능 분석은 컴포넌트 수준의 최악 성능 분석을 포함하는 문제이다. 최근에 프로세서의 수와 태스크 수가 계속 증가하는 추세에 있으므로 실용성 있는 시스템 수준의 성능 분석 기술은 반드시 확장성을 가지고 있어야 한다.

최악 성능 분석이 어려운 이유는 시스템에서 수행되는 태스크들이 모두 최악 수행시간을 가진다고 해서 시스템의 성능이 최악이 되는 것이 아니기 때문이다.

이러한 스케줄링 어노말리 현상은 이미 잘 알려져 있으며 [1] 그림 2는 스케줄링 어노말리 현상의 단순한 예를 보여주고 있다.

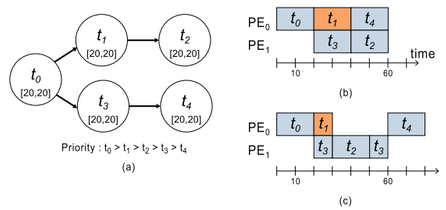


그림 2. 스케줄링 어노말리 예제 (a) 태스크 그래프 예제
(b) 최악 수행시간 기반 스케줄 (c) 최악 응답 시간을 갖는 스케줄

이 예제는 총 5개의 태스크로 이루어져 있고 태스크 t_0, t_2, t_3, t_4의 경우 수행시간이 20으로 고정되어 있다. 반면에 태스크 t_1은 수행시간이 10에서 20까지 가변적인 태스크이다. 태스크 t_1, t_3는 태스크 t_0이 끝난 뒤 수행할 수 있고, 태스크 t_2, t_4는 각각 태스크 t_1, t_3가 끝난 뒤에 수행되는 예제이다. 그리고 태스크 t_0, t_1, t_4는 PE_0에 할당되어 있고 태스크 t_2, t_3은 PE_1에 할당되어 있다. 태스크의 우선순위 관계가 그림 2(a) 에 표시되어 있다.

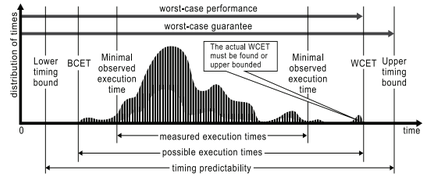
이 예제에 대하여 모든 태스크가 각각의 최악 수행시간인 20일 때의 스케줄을 만들면 그림 2(b)와 같이 응답시간이 60이다. 그러나 이 예제의 실제 최악 응답시간은 태스크 t_1의 수행시간이 최악이 아닌 경우에 발생한다.

그림 2(c)는 t_1의 수행시간이 10일 때 응답시간이 80인 모습을 보여준다. 이 예제를 통해 알 수 있듯이 태스크 별 수행시간이 가변인 시스템에 대해서는 태스크 수행시간의 범위를 모두 탐색해야만 정확한 최악 응답시간을 얻을 수 있다.

최악 성능을 알아내기 위한 일반적인 방법은 시뮬레이션 방법과 측정에 의존하는 것이다. 시스템의 행태에 영향을 주는 입력 값을 변화시키면서 시스템의 최악 응답을 시뮬레이션을 통해서, 혹은 프로토타이핑 실험을 통해서 예측한다.

이러한 방법으로 최악 성능을 얻기 위해서는 실제로 발생할 수 있는 모든 가능성을 다 찾아서 실험으로 재현해야 한다. 하지만 일반적으로 발생할 가능성의 수는 무한하므로 이 방법으로 최악 성능을 예측하는 것은 한계가 있다.

그림 3은 이러한 한계점을 예시로 보여준다. 최악수행시간이 아주 특별한 경우에 발생하는 경우 실험적인 방법으로 구한 최악 수행시간은 그보다 작다. 이러한 단점을 극복하기 위해서 일반적으로 실험으로부터 얻은 결과보다 더 큰 수행 시간을 기준으로 시스템을 설계하곤 하는데, 이는 시스템의 사양을 필요 이상으로 과도하게 책정함으로써 시스템의 안정성을 보장하려는 것이다. 이때, 어느 정도 과도하게 사양을 결정해야 하는지에 대한 문제가 남는다.



Courtesy by R.Wilhelm et al., ACM Trans. Embed. Comput. Sus, 2007.

그림 3. 최악 성능의 측정치와 예측치의 비교

시스템의 복잡도가 증가함에 따라 발생 가능한 경우의 수는 폭발적으로 증가하기 때문에 그만큼 과예측의 크기가 폭발적으로 증가하게 되므로 시스템의 안정성을 보장하기 위해서는 다른 방법이 필요하다. 이에 분석적인 방법으로 최악 성능을 예측하는 연구가 최근에 활발히 이루어지고 있다.

분석적인 방법의 경우 정확한 최악 시간을 구하는 것이 아니라, 최악 응답시간의 상한값(Upper bound)을 계산한다. 가능한 모든 경우에 대한 응답시간이 분석 결과보다 작음을 보장하는 상한을 정하도록 하는데, 과예측을 최소화하는 것이 중요한 문제가 된다.

시스템 수준에서 최악 성능을 예측하는 분석적인 방법은 크게 통합적인 방법(holistic approach)과 조합적인 방법(compositional approach)로 구분할 수 있으며 두 접근법에 근거한 다양한 연구들이 수행되고 있다. 통합적인 방법은 각 컴포넌트 내부에서 발생

하는 태스크 간의 간섭과 통신망에서 일어나는 간섭을 한꺼번에 모두 고려하여 분석하는 것으로 다양한 기법이 존재한다.

먼저 컴포넌트 기반 최악 성능 분석기법을 확장한 연구들이 있다. 1994년도에 발표된 태스크의 수행시간 지연에 대한 비관적인 시나리오를 바탕으로 최악 수행시간을 계산하는 K. Tindell et. al.[2]의 연구가 이 기법의 시초라 할 수 있다.

이 기법은 태스크 간의 의존 관계와 가변 수행시간을 고려하지 않았고, 선점형 스케줄링만 고려하였으며 태스크들이 모두 한 시점에 릴리스(release) 된다는 가정을 하여 많은 제약점을 가지고 있었다. 그 이후에 한계점을 보완한 다양한 분석법이 개발되었으나 여전히 분석할 수 있는 시스템에 대한 한계를 가지고 있다 [3][4].

통합적인 방법으로 정확한 최악 성능을 분석하는 기법으로 모델 체킹에 근거한 기법이 제안되어 스웨덴 웁살라 대학에서 Uppaal[5]이라는 도구로 발표되었다. 모델 체킹 방식은 시스템에 대응하는 Timed Automata를 구성하여 쿼리를 통해 스케줄링의 특성을 알 수 있으며 반복적인 쿼리를 통해 정확한 최악 응답시간도 찾도록 하는 구조이다.

그러나 시스템에 대응되는 Timed Automata를 구성하는 것이 매우 어렵고, 시스템이 복잡해질수록 Timed Automata의 복잡도가 폭발적으로 증가하는 단점이 있다. 아울러 분석시간 또한 지수 함수적으로 증가하는 단점이 있다.

조합적인 분석법은 컴포넌트 프로세서별로 분석을 순차적으로 수행하는 기법으로 MPA[6]와 SymTA/S[7]가 대표적이다. 그림 4에 조합적인 성능 분석기법의 개념을 도시하였다. 이 기법에서 핵심적인 사항은 컴포넌트 간에 전달되는 이벤트를 어떻게 명세 하는가에 관한 것이다. MPA는 이벤트의 도착 커브(arrival curve)와 서비스 커브(service curve)를 정의한다.

도착 커브는 임의의 시간 간격 내에 도착할 수 있는 이벤트의 상한과 하한을 그래프로 표시한 것이며, 서비스 커브는 컴포넌트가 태스크를 실행할 수 있는 대역폭의 상한과 하한을 그래프로 명시한 것이다. 각 컴포넌트는 두 커브 입력을 받아서 실시간 대수(Real-time Calculus)라고 불리는 수학적인 연산을 통해서 다음 단에 전해 줄 도착 커브와 태스크를 수행하고 남는 서비스 커브를 계산한다.

즉 컴포넌트간 이벤트의 전달이 도착 커브로 명세 된다. 반면에 SymTA/S는 이벤트 스트림을 (*p, j, d*) 튜플로 모델한다. 여기서 *p*는 주기, *j*는 최대 지터, *d* 는 이벤트 간 최소 거리이다. 각 컴포넌트에서는 주기적으로 도착하는 이벤트를 바탕으로 기존의 응답시간 분석기법이나 비지윈도우 기법을 사용하여 최악 수행시간을 분석하고 그 결과로 생성되는 이벤트 스트림을 다시 (*p, j, d*) 튜플로 표현한다.

각 프로세서에 대해 입력 이벤트 스트림이 프로세서 내 태스크의 특성을 반영하여 출력 이벤트 스트림이 되고 그에 이어지는 프로세서에 다시 입력 이벤트 스트림으로 주어진다. 최대 지터 값(*j*)이 주기(*p*)보다 크면 이벤트가 한꺼번에 몰리는 경우도 명세할 수 있다.

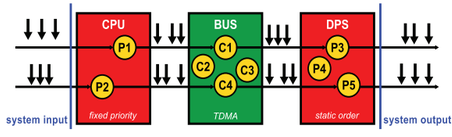


그림 4. 조합적인 최악 성능 분석 기법의 개념

MPA와 SymTA/S 모두 분석 시간이 매우 짧고 시스템의 복잡도가 증가할 때에도 수행시간의 증가 속도가 느려 확장성이 좋은 장점이 있다. 따라서 빠르고 대략적인 분석을 하기에 좋은 특성을 가진다. MPA는 Matlab/SIMULINK에 부가적인 기능으로 포함되어 상용화된 기술이고 SymTA/S는 독일의 Symtavisioin사에 의하여 상용화되어 자동차 응용에 적용되고 있다.

그러나 두 방법 모두 모듈별로 계산하는 과정에서 다른 모듈과의 의존 관계를 고려하지 않기 때문에 최악 응답시간 분석 결과는 과예측되는 경향을 보인다. 또한, 과예측의 정도가 크고 얼마나 과예측이 되는지의 상한도 정해지지 않는다는 단점이 있다.

서울대학교 통합설계 및 병렬처리 연구실(CAP 연구실)에서는 STBA(schedule time bound analysis) 로 명명하는 새로운 기법을 개발하고 있다[8]. 이 기법은 태스크가 수행될 가능성이 있는 시간 범위를 스케줄링을 수행하면서 분석하는 통합적인 방법이므로 조합적인 방법에 비해 과예측의 정도를 획기적으로 줄일 수 있다는 장점이 있다. 반면에 모델체킹 방법과 달리 모든 경우의 수를 다 따지지 않아도 되기 때문에 분석의 속도를 획기적으로 낮추고, 조합적인 방법에 버금가는 분석 속도를 얻을 수 있다.

제안하는 방법을 그림 5의 예를 가지고 간략하게 설명한다. 이 예제에는 2개의 응용 프로그램 (T_0, T_1) 이 각각 2개의 태스크로 구성되어 있다. 4개의 태스크가 2개의 프로세서 (PE0, PE1)에 그림과 같이 매핑되어 있으며 태스크의 우선순위도 주어져 있다.

각 태스크의 수행시간은 [BCET,WCET]의 쌍으로 그림에 표시되어 있다. PE0 프로세서는 선점형 스케줄링을 채택하고 PE1 프로세서는 비선점형 스케줄링을 채택하고 있다. 두 응용 프로그램이 모두 시간 0에서 수행을 시작한다고 가정하고 주기는 100이라고 하자.

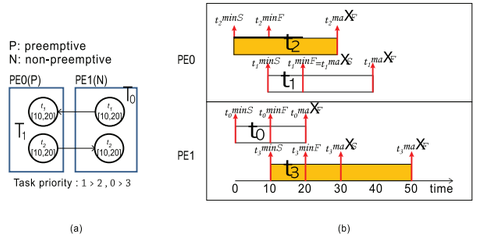


그림 5. STBA 기법 (a) 예제 시스템 (b) 분석 결과

제안하는 기법에서는 각 태스크가 스케줄될 수 있는 (T^{minS}, T^{maxS}), (T^{minF}, T^{maxF}),범위를 두 쌍의 튜플로 표시한다. 여기서 T^{minS}와 T^{maxS}는 태스크 T가 수행을 시작할 수 있는 가장 이른 시간과 가장 늦은 시간을 각각 표시한다. 마찬가지로 T^{minF}와 T^{maxF}는 태스크 T가 수행을 끝낼 수 있는 가장 이른 시간과 가장 늦은 시간을 각각 표시한다.

각 태스크가 스케줄 되는 범위를 계산하기 위해서 그림 5(b)에 도시하는 바와 같이 실제로 태스크를 프로세서에 매핑하고 스케줄을 하는 과정을 거친다. 태스크를 각 컴포넌트 프로세서에 스케줄 할 때에 태스크의 우선순위와 선후 관계를 고려하게 된다.

위의 경우 시간 0에서 수행 가능한 태스크는 PE0의 경우 T_2밖에 없고 PE1의 경우 T_0밖에 없다. 이 태스크를 스케줄하면서 (T^{minS}, T^{maxS}), (T^{minF}, T^{maxF})의 값을 구한다. 이들 태스크가 수행을 끝내게 되면 T_1과 T_3가 수행가능하게 되므로 이들 태스크의 스케줄 가능 범위를 구한다. 이렇게 스케줄을 1회 수행하고 난 뒤에 스케줄을 다시 점검한다.

처음 스케줄을 할 때에는 T_1의 스케줄 범위에 대한 정보가 없었지만, 2번째 스케줄을 할 때에는 T_1의 스케줄 범위에 대한 정보를 참고해서 T_2의 스케줄 범위를 다시 계산한다. T_2의 스케줄 범위가 조정되면 선후 관계에 있는 T_3의 스케줄 정보도 갱신되어야 한다. 이런 식으로 모든 태스크의 스케줄 범위가 수렴될 때까지 스케줄을 반복한다. 이처럼 제안하는 방법은 태스크의 스케줄 범위를 보수적으로 계산하는 것이므로 태스크 T_2와 선후관계가 있는 태스크 T_3의 스케줄 가능 범위가 매우 넓게 정의되는 것을 볼 수 있다.

이 기법은 현재 단일코어 프로세서들이 버스로 연결된 간단한 구조에 대하여 개발되었는데 향후 멀티코어 프로세서들이 NoC로 연결된 구조와 동적인 특성을 가지는 응용에 대한 분석법으로 확장할 예정이다.

Reference

[1] R. L. Graham, "Bounds on multiprocessing timing anomalies," SIAM J. Appl. Math., 17(2), pp. 416-429, Mar. 1969.

[2] K. Tindell and J. Clark, "Holistic Schedulability Analysis of Distributed Hard Real-time Systems," Microprocessing and microprogramming, Vol. 40, pp. 117-134, April, 1994.

[3] J. C. Palencia and M. G. Harbour, "Schedulability Analysis for Tasks with Static and Dynamic Osets," Proceedings of RTSS, pp. 26-37, December, 1998.

[4] F. Slomka, J. Zant, and L. Lambert, "Schedulability analysis of heterogeneous systems for performance message sequence chart," Proceedings of CODES, pp. 91-95, March, 1998.

[5] A. Brekling, M. R. Hanse., and J. Madsen, "Models and formal verification of multiprocessor system-on-chips," J. Logic Algebraic Program., 77(1-2), pp. 1-19, Sep.-Oct. 2008.

[6] L. Thiele, E. Wandeler, and S. Chakraborty, "Performance analysis of multiprocessor DSPs: A stream-oriented component model," IEEE Signal Process. Mag., 22(3), pp. 38-46, May 2005.

[7] K. Richter, M. J., and R. Ernst., "A formal approach to MpSoC performance verification," IEEE Computer, 36(4), pp. 60-67, 2003.

[8] J. Kim, H. Oh, J. Choi, H. Ha, and S. Ha, "A Novel Analytical Method for Worst Case Response Time Estimation of Distributed Embedded Systems," Proceedings of DAC, June, 2013.

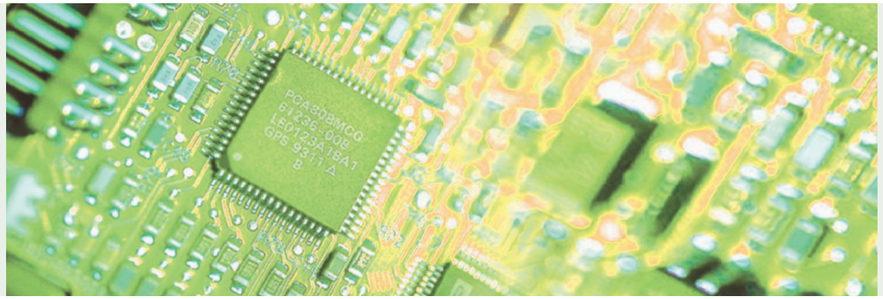
전자파 및 전력 소모량 측정 등 다양한 부채널 분석을 통한 암호모듈 분석 소개

고려대학교 정보보호대학원(CIST)

김현민 박사과정
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
E-mail : willguts@korea.ac.kr
crypto.korea.ac.kr

고려대학교 정보보호대학원(CIST)

홍석희 교수
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
E-mail : shhong@korea.ac.kr
http://crypto.korea.ac.kr



부채널 분석을 통한 암호 모듈 분석

스마트카드나 RFID 같은 소형 전자 장비의 사용이 늘어나면서 이러한 장비들에 대한 물리적인 보안 문제가 중요한 이슈로 떠오르고 있다. 특히, 부채널 분석을 이용한 방법은 칩에 손상을 입히지 않고 칩 안에 저장된 비밀정보를 얻어내는 공격방법이기 때문에 관련 공격에 대한 대응책이 고려되어야 한다.

즉, 스마트카드의 활용분야가 확대되면서 IC칩의 물리적인 안전성에 대한 관심이 높아지고 있다. 그에 따라 스마트 카드에서 동작하는 암호 알고리즘과 프로토콜 자체가 이론적으로 안전하더라도 실제로 구현된 방법에 따라 위협적인 공격이 가능하다는 사실이 알려졌다.

대표적으로 IC 칩에 내재한 암호 알고리즘에 대한 부채널 분석 공격이 국내외에서 많이 연구되고 있다. 실제로 스마트 카드는 금융(직불, 신용, 전자화폐), 통신(전화카드, 이동통신카드), 교통(교통카드), 의료(의료보험카드), 전자 상거래(비밀키 저장), 보안(인터넷, PC 보안 솔루션, 인증서 저장)과 같이 많은 분야에서 사용되고 있기 때문에, 비밀 정보가 노출될 경우에 개인 및 단체가 입을 수 있는 피해가 막대하다.

따라서 현재 널리 사용되고 있는 스마트 카드에 대해 최근 연구되고 있는 부채널 분석 방법인 전력 분석 공격과 전자파 분석 공격을 적용하여 안전성을 검증하고, 이를 바탕으로 향후에 부채널 분석 공격에 안전한 스마트 카드를 개발하는 것이 필요하다.

우리나라에서 제조된 제품이라 하더라도 현재 스마트 카드와 관련된 안전성 검증, 특히 부채널 공격에 대한 검증은 대부분 유럽에서 이루어지고 있는 실정이다. 즉, 우리나라에서는 아직 스마트 카드의 안전성을 검증할 수 있는 기술적인 기반이 마련되어 있지 않은 것이 실정이다. 우리나라는 스마트 카드 주요 생산국 중 하나이며 앞으로 이것은 더욱 가속화될 전망이다.

우리나라가 독자적인 스마트 카드 경쟁력을 갖추기 위해서는 장치 설계뿐만 아니라 보안 메커니즘의 설계 및 안전성 검증 기술까지 갖추어야 한다.

특히 본 컬럼에서는 스마트카드에 많이 사용되는 타원곡선 암호 알고리즘에 대한 전력 분석 공격 및 전자파 분석 공격의 최신동향에 대해 알아보고 이러한 공격을 통해 알고리즘의 안전성을 분석 및 평가하는 방법에 대해 설명하고자 한다.

그림 1. 부채널 분석

부채널 분석을 위한 실험 장비 구성

부채널 분석을 위해 본 연구실에서 구비 중인 장비는 다음과 같다.

1) 오실로스코프(Lecroy社의 6000 Series인 LSA1225)

2) 스펙트럼 분석기(ADVANTEST社의 R3267) : 스펙트럼 분석기를 사용하여 노이즈를 제거하고, 주파수 도메인 상에서 해당 주파수에서의 전력 또는 전자파 값을 나타낸다.

3) 카드 리더기(Gemalto社의 PC Twin과 MicroPross社의 MP300)Gemalto사의 PC Twin 카드 리더기의 특성 : EEPROM에 코드를 다운로드 할 때 File Downloader 프로그램과 호환이 된다. MicroPross 사의 MP300 의 특성 : 카드리더기로 제공하는 MP-scope툴을 이용하여 스마트 카드에 APDU 명령어를 보내고 그에 따른 출력 값을 추출할 수 있다. 따라서 공격에 필요한 APDU 명령어에 해당하는 연산에 대한 전력 소비량 또는 전자파 방사량 파형을 얻을 수 있어 전력 분석 및 전자파 분석에 적합한 카드리더기이다.

4) EM Probe(LANGER EMV-Technik GmbH 社의 Near Field Probe set LF 1과 Preamplifier PA 303) : 소비 전자파 분석 실험에서 전자파 방사량을 측정하기 위하여 사용한다. Near Field Probe set LF 1는 네 개의 EM Probe (LF-R 400, LF-U 2.5, LF-U 5, LF-B 3)를 포함하며, 전자파 방사량을 증폭시켜주는 장비인 Preamplifier를 함께 사용하여 전자파 방사량을 측정한다. 다음 그림 2는 부채널 분석에 일반적으로 많이 사용하는 장비에 대해 나타내었다.

그림 2. 부채널 분석 장비

부채널 분석을 위한 실험 장비 설치

스마트 카드에 대한 부채널 분석을 위한 기본적인 장비는 그림 3과 같이 설치한다.

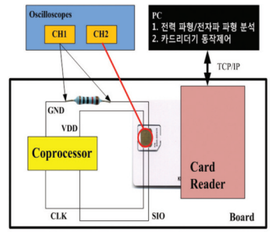


그림 3. 실험 장비 셋팅

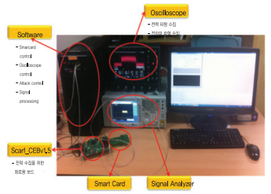


그림 4. 부채널 분석을 위한 실험 환경 구성

1) 본 연구실에서 갖춘 PC Twin 카드리더기는 PC와 USB port로 연결하여 File Downloader 프로그램으로 EEPROM에 코드를 다운로드 하고, MP300 카드 리더기는 PC와 TCP/IP 통신을 한다.

2) 분석 타켓이 되는 칩과 카드리더기의 연결을 위해 PCB 보드와 칩을 연결한다.

3) 타겟 칩에서 사용되는 단자는 GND, VCC, CLK, IO 단자를 사용한다. VCC 단자는 칩이 동작하기 위한 전원이 공급되는 단자이고, 카드리더기에서 제공하는 전원을 사용하지 않고 외부에서 전원을 공급하여 분석할 경우 사용된다. CLK 단자 역시 카드리더기에서 제공하는 클럭이 아닌 외부 클럭을 사용할 경우에 사용된다.

4) 사용되는 4개의 단자를 스마트 카드 리더기와 연결하기 위해서 PCB 보드와 연결한다. 이 때 Passive Voltage Probes를 사용하기 때문에 사용되는 전력 소모량을 측정하기 위해서는 PCB 보드와 GND 단자와 칩의 GND 단자 사이에 1Ω~50Ω의 저항을 연결한다.

5) 전력 소모량에 대한 파형을 수집하기 위하여 실험 장비의 접지들은 모두 PCB 보드의 GND와 연결한다.

6) 오실로스코프는 2개의 채널을 이용한다. CH1의 경우는 칩이 동작하는 동안의 소비 전력을 측정하기 위한 것이고, CH2의 경우에는 PCB 보드에서 발생하는 전자파 방사량을 측정하기 위한 것이다.

전력 분석 및 전자파 분석 방법 소개

전력 분석

1) 단순 전력 분석

단순 차분 분석(Simple Power Analysis, SPA)는 하나의 전력 파형을 이용하여 소비전력 신호를 통해서 연산의 수행 패턴을 알아낼 수 있을 경우에 사용하는 전력 분석 방법이다. 이는 연산이 실행되거나 데이터의 이동 또는 저장되는 순간에 소비되는 전력량이 늘어나는 성질을 통하여 개인키를 알아낼 수 있는 경우는 극히 드물다.

단, SPA를 통해서 실제 타겟이 되는 연산이 일어나는 시점을 알아내서 분석에 용이하게 하는 효과를 가지고 올 수는 있다. 따라

서 이러한 SPA 분석을 통해서 다음에 언급할 DPA, CPA가 좀 더 수월해지는 것을 알 수 있다.

2) 차분 전력 분석

차분 전력 분석(Differential Power Analysis, DPA)은 전력 파형의 형태만을 통해서 개인키를 알아내는 SPA와 달리 전력 파형을 공격자가 예측한 키 값에 따라 분류하여 차분(Difference) 전력을 계산하고 이를 이용하여 분석하여 키를 찾는 기법이다. 일반적으로 DPA는 알고리즘의 특성에 따라 다양한 방법으로 적용 가능하며 가장 널리 사용되는 전력 분석의 방법 중 하나이다.

3) 상관 계수 전력 분석(Correlation Power Analysis, CPA)는 DPA와 상당히 유사한 분석 기법으로 상관계수를 이용하여 장비의 비밀 정보를 찾는다. 즉, 공격자가 추측한 값에 따라 중간값을 예측하고 전력 파형의 상관계수를 통해 키를 찾는 방법이다. 그러므로 옳은 키를 예측했을 경우에는 상관계수가 높아지며 틀린 키를 예측했을 경우는 상관계수가 낮아진다. 이에 암호 연산과 관련해서 상관계수가 높아지는 시점을 피크라고 정의하며 이를 통해 옳은 키와 틀린 키를 구별하여 개인 키를 찾아낼 수 있다.

전자파 분석

전자파의 방사는 Control, I/O, 데이터의 처리 또는 디바이스의 여러 부분으로의 연속된 데이터의 흐름에서 발생한다. 전자파 방사량은 활성화되어 있는 게이트(Active gate)의 물리적 특성에 모두 의존하게 되므로 하나의 전자파 센서에는 다른 타입의 많은 전자파 신호가 측정된다. 즉, 전자파 방사량의 측정에서 디바이스의 물리적, 전기적 특성에 기초한 전자파 방사(Direct emanation)뿐만 아니라 여러 연결장치 등에 의하여 발생하는 전자파 방사(Unintentional emanation)가 포함된다. 따라서 이들 전자파 신호는 독립적으로 분리될 수 있고 그 특성을 이용하여 분석된다. 이는 모든 활성화된 게이트에 의하여 소비되는 전력량이 집적되어 측정되는 전력 분석과 차별되는 특성이다. 하지만 비오-사바르의 법칙(Bio-Savart's Law)에 의하여 전자파 분석은 전력 분석과 유사한 방법으로 분석이 가능함을 알 수 있다.

1) 비오-사바르의 법칙(Bio-Savart')

이 법칙은 정상전류가 흐르고 있는 도선 주위의 자기장의 세기를 구하는 법칙이다. 이 법칙을 이용하면 도선 밖의 한 점에서의 자기장의 세기를 구할 수 있다. 즉, 이 법칙을 이용하면 도선 밖의 한 점에서의 자기장의 세기는 회로 안의 작은 면적의 자기장의 벡터 합으로써 구할 수 있다. 전자파 분석에서 사용하는 EM Probe의 지름이 r일 때, 자기장의 세기 B를 구하는 공식은 다음과 같다.

$$B = \frac{\mu_0 I}{2\pi r}$$

이때, I는 전류의 세기, μ_0는 자기 상수(Magnetic Constnat)이다. 즉, 전자파의 세기는 전류의 세기에 비례하고, EM Probe의 지름에 반비례함을 알 수 있다. 따라서 전자파 분석에서 사용하는 EM Probe의 지름이 일정하면 전자파의 세기는 전류의 세기에 비례하는 것을 알 수 있다. 따라서 옴의 법칙(Ohm's Law)에 의하여 I = V/R을 만족하고 전자파의 세기를 다음과 같이 나타낼 수 있다.

$$B = \frac{\mu_0 V}{2\pi r R}$$

따라서 전자파 분석에서 필요한 파형을 수집할 때, 일정한 저항을 사용하므로 전자파의 세기는 전력의 세기에 비례함을 알 수 있다. 즉, 전자파 파형은 전력 파형과 유사한 성질을 가진다.

전자파 분석에는 크게 단순 전자파 분석(Simple Eletro Magnetic Analysis, SEMA), 차분 전자파 분석(Differential Eletro Magnetic Analysis, DEMA), 상관계수를 이용한 전자파 분석(Correlation Electro Magnetic Analysis, CEMA)등의 방법이 제안되었다. 비오-사바르의 법칙에서 전자파 파형과 전력 파형의 유사한 특성에 의하여 접근하는 방식은 전력 분석과 유사하다. 즉, SEMA, DEMA, CEMA는 각각 SPA, DPA, CPA와 분석 방법이 비슷하고 분석 결과 또한 유사한 성질을 가진다.

전력 소비 및 전자파 방사 모델

전력 분석(또는 전자파 분석) 공격 방법은 공격이 되는 대상이 전력을 소비(또는 전자파 방사)하는 방법에 따라 다르게 적용된다. 즉, 전력 분석(또는 전자파 분석) 공격을 시도하기 전에 반드시 공격의 대상이 되는 장비가 전력을 소비(또는 전자파 방사)하는 방법을 파악해야 한다.

장비들은 전력을 소비(또는 전자파 방사)하는 방법에 따라 해밍 웨이트 모델(Hamming weight model)과 해밍 디스턴스 모델(Hamming distance model)으로 나누어진다. 비오-사바르의 법칙에 의해 전력 소비 모델과 전자파 방사 모델은 유사하므로 본 절에서는 두 모델의 전력 소비 방법에 대해 설명한다.

해밍 웨이트 모델(Hamming weight model)

m-bit microprocessor에서 이진 데이터 $x = \sum_{j=0}^{m-1} x_j 2^j$ (x_j :0 or 1)에 대한 해밍 웨이트(Hamming weight)란 x_j들 중 1의 개수를 뜻하며 본 컬럼에서는 W(x)로 이 값을 정의한다. 이때, 데이터 버스를 흐르는 데이터의 해밍 웨이트에 따라 전력을 소비하는 장비들을 해밍 웨이트 모델이라 말한다. 즉, 장비에서 x란 데이터가 데이터 버스를 흐를 때의 전력 소비량 C가 주어진 상수 a,b에 대하여 aW(x)+b와 유사할 때, 이 장비를 해밍 웨이트 모델을 따른다고 한다.

aW(x)+b의 식에서 a,b의 값은 장비에 따라 달라지는 값으로, 공격 대상인 어떠한 장비가 주어졌을 때 이 값을 사전에 알아내는 것은 공격자의 공격을 상당히 용이하게 할 수 있다. 즉, 공격자가 이 값을 사전에 알아낸다면 소비된 전력을 통해 이 시점에서 데이터 버스를 흐르 데이터의 해밍 웨이트를 알아낼 수 있다. 물론 이 정보를 이용해 정확한 데이터의 값을 알아낼 순 없지만, 이러한 정보가 누적될 경우 공격자는 충분히 장비의 비밀 정보를 알아낼 수 있다.

해밍 디스턴스 모델

두 데이터 x와 x' 의 해밍 디스턴스(Hamming Distance)란 비트 별로 비트의 값이 다른 위치의 수를 뜻하며 이 값은 W(x xor x')와 같다. 대표적으로 CMOS와 같은 디바이스에서의 전력 소비는 데이터 버스를 흐르는 전후 데이터의 해밍 디스턴스에 의존하며, 이러한 장비들을 해밍 디스턴스 모델이라 한다. 해밍 디스턴스 모델에서 데이터의 변화에 따른 소비 전력은 다음 표와 같다. 이때 δ는 0과 1사이의 고정된 상수 값이다.

표 1. 해밍 디스턴스 모델

Transitions	Power
0 -> 0	0
0 -> 1	1
1 -> 0	$1-\delta$
1 -> 1	0

위 표의 x값은 해밍 디스턴스 모델에서 디바이스 또는 장비마다 달라지는 값이다. 해밍 웨이트 모델에서 a, b의 값을 사전에 조사한 것과 마찬가지로 이 x의 값을 사전에 알아내는 것은 공격자의 공격을 상당히 용이하게 할 수 있다.

전력 분석 및 전자파 분석 동향

부채널 공격 방법 중 전력분석 공격에서 강력한 분석 방법으로 알려진 템플릿 공격에 대하여 간단히 설명하고, 실제 템플릿 공격을 사용해서 실제 사용 중인 스마트 카드에 대한 분석 사례인 David Oswald와 Christof Paar의 "Breaking Mifare DESFire MF3ICD40: Power Analysis and Template in the Real World" 논문에 소개된 내용을 살펴보겠다.

template 분석 소개

1) 전력 분석 공격 vs 템플릿 공격

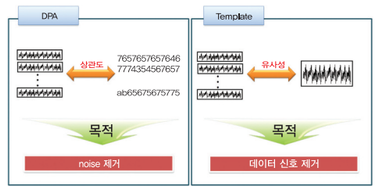


그림 5. 전력 분석 공격 vs 템플릿 공격

2) 템플릿 분석 시 고려사항

부채널 정보에서 노이즈의 데이터 종속성은 확률분포(다변량 Gaussian 분포)에 의해 영향을 받는다. 비밀 정보가 포함된 데이터에 종속된 노이즈를 확률분포로 모델링 하여 템플릿(template)을 생성한다.

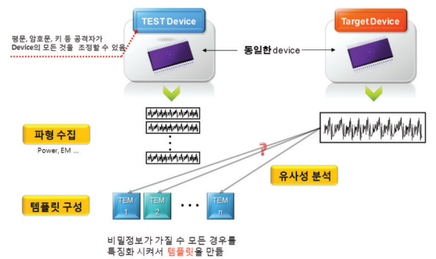


그림 6. 템플릿 생성

3) template 이란?

비밀정보에 대한 확률 분포(가우시안 분포)를 의미한다.

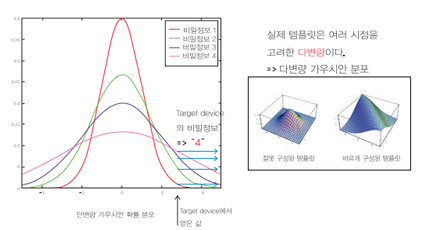


그림 7. 템플릿의 개념

4) template 구성단계

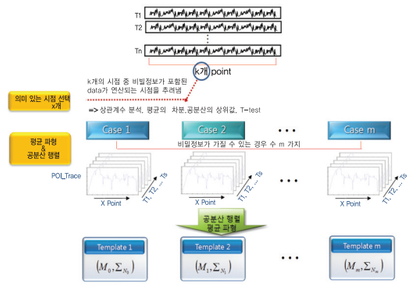


그림 8. 템플릿의 구성 단계

5) 템플릿에 대한 유사성 분석 단계(Matching)
Target device에서 얻은 부채널 정보와 미리 구성해 놓은 템플릿과의 유사성을 확률로 계산 : 가장 유사한 템플릿의 정보를 통해 Target Device의 비밀정보를 얻는다.

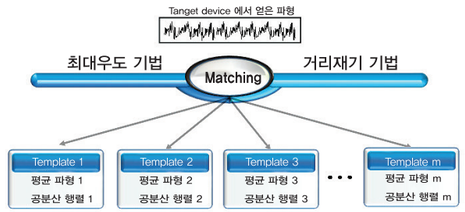


그림 9. 템플릿에 대한 유사성 분석

템플릿 분석을 이용한 실제적인 공격 사례

2011년 CHES(workshop on Cryptographic Hardware and Embedded System)에서 독일 Ruhr 대학의 Christof Paar의 연구그룹에 의해서 전력분석과 템플릿 공격방법을 이용한 스마트카드 Mifare DESFire MF3ICD40에 대한 실제적인 공격사례가 발표되었다.

1) Mifare DESFire MF3ICD40의 스펙 및 구성도
• 2002년 Philips에 의해서 개발(현 NXP)
• 데이터 암호화와 인증을 위해서 112bit key를 가진 3DES co-processor 엔진을 사용
• 4kB non-volatile 메모리 사용
• Asynchronous 8051 기반의 프로세서 사용

2) Mifare DESFire MF3ICD40 칩 구성도 및 기본 인증 프로토콜

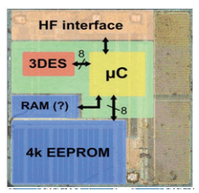


그림 10. 칩 구성도

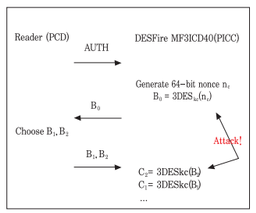
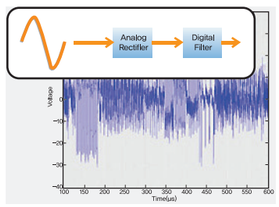
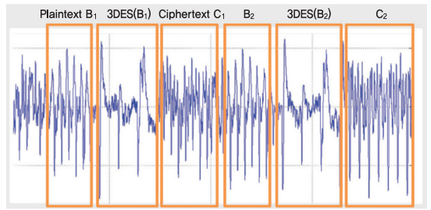


그림 11. 기본 인증 프로토콜

3) Mifare DESFire MF3ICD40에 대한 템플릿 공격
a. 파형 수집



b. Mifare DESFire의 동작 위치 파악



c. leakage 정보 획득
– leakage 1: Bitwise Hamming Distance of round 0–>1 of DES_k1(B), freq. Domain
– leakage 2: Hamming Weight DES_k1(B), time Domain
– leakage 3: HD round 0–>1 of DES_k2^(–1), freq. Domain
– leakage 4: HW of ciphertext C
d. 키 k1, k2를 다음 순서로 찾는다.
– DES1, round1: max. 48/56 bit of k1(250k traces)
– Full state after DES1: remaining bits of k1(150k traces)
– DES2, round2: max. 48/56 bit of k2(250k traces)
– Ciphertext: remaining bits of k2(< 2000 traces)

Mifare DESFire MF3ICD40은 템플릿 공격으로 250k traces를 가지고 7시간 안에 모든 키 값을 복구해낼 수 있었다. 또한, 키 복구에 드는 전체 비용은 약 2500 USD로 수행되었다. 이 논문에서 보인 것처럼 매우 짧은 시간에 적은 비용으로도 Mifare DESFire MF3ICD40가 템플릿 공격에 안전하지 못함을 보임으로써 현재 사용하는 스마트카드가 결코 안전하지 못함을 보였다.

결론

기존에는 암호 및 보안에 관한 연구가 주로 수학과 컴퓨터 공학에 머물러 있다고 많이 생각되었다. 하지만 기술이 발전하고 사용하는 소형 장비 등을 이용한 결제 수단 등이 등장하면서 점점 더 이러한 장비들의 취약점을 이용한 다양한 공격방법들이 개발되면서 하드웨어에 대한 보안 이슈가 점점 더 많아질 것이라고 확신한다. 특히, 스마트카드 등에 대한 부채널 분석은 점점 더 개인의 사생활을 위협할 만큼 큰 위험요소로 자리 잡고 있다.

이렇게 많은 위험요소가 존재함에도 불구하고 실제 국내에서는 관련 연구가 특정 몇몇 연구그룹이나 학교에서만 주로 이루어지고 있는 실정이다. 따라서 이러한 분야에 대한 연구가 좀 더 다양한 곳에서 이루어진다면 현재 유럽이나 미국, 일본 중심의 부채널 분석 방법 및 개발에 대해서 한국에서도 좋은 연구 결과들이 많이 나올 수 있을 것이다.

Reference

1) Timing Attacks on Implementations of Diffie–Hellman, RSA, DSS, and Other Systems, P. Kocher et al.

2) Power Analysis Attacks ? Revealing the Secrets of Smart Cards

3) EM Side–Channel Attacks on Commercial Contactless Smartcards using Low–Cost Equipment

4) Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World, David Oswald and Christof Paar

Prime 2013은 2013년 6월 24일부터 27일까지 오스트리아 빌라흐에서 개최되었다. 정상 수준의 산업계와 학계 연구진들이 기술위원으로 위촉되었고 연구 트렌드와 발전방향에 관한 훌륭한 초청강연들도 준비되어 있었다. DC와 RF뿐만 아니라 아날로그에서 디지털까지 전자공학의 거의 모든 분야 및 애플리케이션까지 망라하여 우수한 논문들이 많이 발표되었다. 본 기고문은 Prime 2013의 Power Management 세션 및 Infinieon의 Plenary Paper에서 소개된 기술 및 동향을 참가 후기 형식으로 정리하였다.

모바일 폰, 태블릿 PC, 노트북 등 다양한 IT 기기들이 소형화되고 효율성, 범용성이 증대됨에 따라 널리 보급되고 있다. 이러한 기기들이 PC, MP3, 카메라 등 다양한 기능을 수용하기 위해서는 전원을 효율적으로 조정하는 Power Management가 필수적으로 요구된다. 구동 전력을 공급하는 기본적인 기능 외에도 전력관리에는 배터리 용량 감지 회로, 배터리 인증, 밸런싱, 외부환경 보호회로 등이 포함된다.

SPECIAL Column I

Prime 2013 참가후기 및 기술 트렌드

Prime 2013은 2013년 6월 24일부터 27일까지 오스트리아 빌라흐에서 개최되었다. 정상 수준의 산업계와 학계 연구진들이 기술위원으로 위촉되었고 연구 트렌드와 발전방향에 관한 훌륭한 초청강연들도 준비되어 있었다. DC와 RF뿐만 아니라 아날로그에서 디지털까지 전자공학의 거의 모든 분야 및 애플리케이션까지 망라하여 우수한 논문들이 많이 발표되었다. 본 기고문은 Prime 2013의 Power Management 세션 및 Infinieon의 Plenary Paper에서 소개된 기술 및 동향을 참가 후기 형식으로 정리하였다.

모바일 폰, 태블릿 PC, 노트북 등 다양한 IT 기기들이 소형화되고 효율성, 범용성이 증대됨에 따라 널리 보급되고 있다. 이러한 기기들이 PC, MP3, 카메라 등 다양한 기능을 수용하기 위해서는 전원을 효율적으로 조정하는 Power Management가 필수적으로 요구된다. 구동 전력을 공급하는 기본적인 기능 외에도 전력관리에는 배터리 용량 감지 회로, 배터리 인증, 밸런싱, 외부환경 보호회로 등이 포함된다.

휴대용 기기들의 특성상 저가격, 소형화를 위해 Power Management는 IC로 구현되고 있는 추세이다. PMIC(Power Management Intergrated Chip)는 다른 칩에 비해 비교적 높은 가격을 형성하고 있으며 상시적으로 전원이 공급되는 포터블이나 모바일 기기에는 필수적으로 사용되는 부품이다. 근래에는 ASIC 또는 ASSP의 형태의 IC 수요가 커지고 있다.

Prime 2013의 세션 W2A(Power Management)에는 총 3편의 논문이 발표되었다. 첫 번째 논문은 piezoelectric energy harvesting에 이용되는 PMIC를 소개하고 있다. 시작 위상 속도와 수확 유효성을 개선하는 것을 목표로 스마트 자가 공급 아키텍처를 적용했고, residual charge inversion과 양방향 저장 토폴로지를 제안했다.

특히 Synchronous electrical charge extraction(SECE)를 기반을 두어 Conversion Scheme이 포괄적으로 연구 되었고 이가 passive interface보다 효율적이었다.

Converter는 특정한 일을 수행하는 하위 시스템으로 구성했다. 이론상으로는 매우 낮은 듀티 싸이클을 가지는 Single inductor가 하나 필요하다. 시동시간을 단축하기 위해서 추가로 캐패시터 CDD가 추가되었고 Power conversion circuit으로 파워를 전달하게 된다.

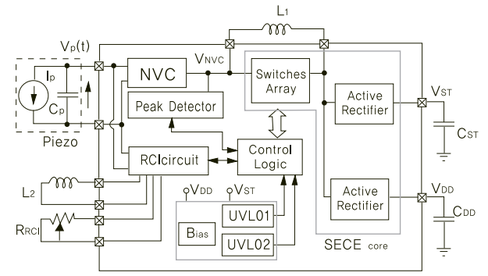


Fig1. Block diagram of the designed converter

에너지 추출을 42% 향상하게 시켰으며 RCI와 AC-DC 컨버터를 0.32㎛ BCD로 구현했다. 회로는 fully-autonomous 했고, 400nW, 2.7V에서 정동작 전류는 150nA를 보였다.

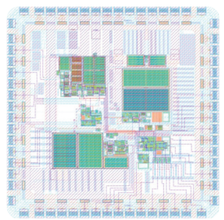


Fig. Layout of the designed IC

전파가 일상에서 정보와 신호를 전달하는데 널리 이용됨에 따라 유선으로 이용되는 통신은 무선으로 점차 대체 되었다. 하지만 주변에는 아직도 케이블이 널려있으며 주로 전력용 케이블임을 알 수 있다. 최근에는 전력을 무선으로 공급하는 시스템이 널리 개발되고 있으며, 학계 및 업계에서 연구가 이루어지고 있다.

두 번째 논문은 자기 공진형 무선전력전송 시스템에서 작동하는 모바일용 배터리 충전회로를 소개하고 있다. 비방사형 중거리 무선 에너지 전송 기술이 최근 관심을 받고 있는 가운데 유도방식보다 원거리에서 충전이 가능한 비방사형 자기 공진 방식의 시스템이 두 번째 논문에서 소개되었다. 송수신단을 비롯하여 스마트 폰의 실제 무선충전이 실험으로 구현되었으며, 고효율의 power recovery scheme이 설계 및 칩으로 구현되었다. 공진형 전력 전송기의 송신부는 source coil과 공진을 일으키는 resonator로 작용하는 Tx coil로 구성된다. Source coil에는 RF Power Generator에 의해 RF 전력이 입력되며 Source coil에서 Tx coil로는 전자기 유도에 의해 전력이 전송된다.

출력을 향상시키기 위해 Matching 회로가 구성되는데 두 단 간의 임피던스 차이를 완충시켜서 신호전력을 최대한으로 전달하기 위해 임피던스 매칭 네트워크를 사용하여 최대 14.1%, 평균 7.21%의 효율증가를 확인할 수 있었다. 칩은 LOCOS 0.35㎛ CMOS 공정을 기반으로 동부하이텍의 BCD 기술을 채택하여 제작되었다.

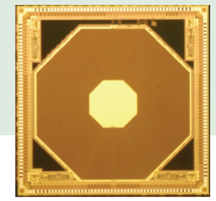


Fig3. Die microphotograph of the integrated chip, size: 5mmX5mm

RF Power generator는 2W의 RF Power를 13.56MHz로 공급했고 최대 전송효율은 송수신 코일 간 거리가 20cm에서 74.3%를 보였다. RFID와 Sensor network와 같은 독립형 무선 시스템의 수요가 증가하면서 로드 회로의 적절한 동작이 가능하게 하는 PMU(Power Management Unit)의 시장 요구도 다각화되고 있다. 무선 시스템의 energy budget은 전형적으로 낮으며 무선전력 전송 역시 이 budget을 사용하는 것을 불가피하게 복잡하게 만든다. 회로의 동작을 지속할 수 있도록 충분한 에너지를 저장시키는 것이 핵심이다.

세 번째 연구는 비용을 저감하고 크기를 줄이면서 퍼포먼스를 개선하는 무선 전력 회로를 제안했다. 2V보다 낮은 전압에서 커패시터에 입사에너지를 저장하는 대신에 저장된 에너지를 높이기 위해 더 높은 전압을 사용했다. 전압과 커패시터를 증가시킴으로 에너지 저장 밀도를 증가시키려 하는 기본적인 접근방법을 채택했는데 저장에너지는 커패시터와 전압의 제곱근에 비례하기 때문에 매우 효과적인 방식이라 할 수 있다.

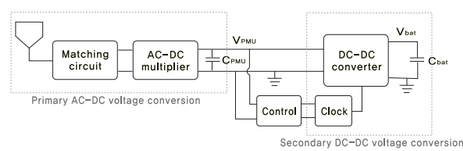


Fig4. Block diagram of the proposed energy storage system

Fig3 에서 볼 수 있듯이 구조는 두 개의 메인 전압 전환 블록과 해당 동작을 위한 컨트롤 블록으로 제안된다. Primary voltage conversion 부분에는 안테나에서의 전압을 System supply voltage VPMU로 상승시키고 정류한다. 이때 이 지점이 Active set-up voltage conversion의 시작점이 된다. Secondary DC-DC voltage conversion은 제어의 용이성, 신뢰성, 저 전력 구동의 특성이 있는 Dickson DC-DC converter를 채택하였다.

Die 크기의 제한 때문에 안테나는 Dipole 형태의 1.8mm의 길이로 적용되었다. 4W의 전력을 등방적으로 방사할 수 있었으며 Vant는 13.9cm에서 100mV이다. AC-DC Multiplier에서 입력 100mV에서 Vpmu를 1.2V까지 발생시키기 위해서 cascaded stage의 수와 구성요소들의 크기를 최적화하였다.

트랜지스터의 크기는 모두 동일하며 W/L 값은 7.2/0.08㎛이다. 전체 23stage가 캐스케이드 되었고 파워효율은 18%에 도달할 수 있었다. AC-DC Multiplier의 입력전압을 높이기 위한 매칭회로가 소개되는데 낮은 quality factor에 기인하여 사용된 CMOS 기술에서 인덕턴스는 2.6nH로 제한된다. 이는 적절한 전력매칭을 하기에는 낮은 수치이기는 하지만 전압 매칭은 집적된 안테나 터미널에 위치한 1.6nH의 인덕터에서 정상 기능을 수행한다.

Infineon Technologies사(社)에서는 Smart Power:From Problem Statement to System Solution이란 제목으로 고전력, 고효율의 인버터를 소개했다. 이 인버터는 SiC(Silicon Carbide) JFET Switch를 기반으로 했으며, 완성된 시스템의 측정값을 소개하며 마무리 지었다. 최종 설계에서 1,000V에 30A를 처리할 수 있으면 최대 효율은 99%였다.

주로 99%의 효율을 위해서는 16~30kHz 사이의 IGBT나 고전압 실리콘 MOSFET이 사용된다. 그러나 스위칭 주파수가 상승할 때, 이를테면 100kHz에서 switching loss는 지나치게 높아지게 되고 이에 SiC를 이용한 JFET가 대안이 될 수 있다. 메인 고전압 파워가 JFET의 소스에 계속 공급이 된다면, 핀치오프 전압에 도달할 때까지 계속 상승할 것이다.

드라이버는 보통 컨트롤러로부터 입력을 받아 두 파워 트랜지스터(JFET와 +MOSFET)에 공급해야하는데, 이 두 파워트랜지스터는 상당히 다른 두 전압에도 연결될 수 있다. 보통은 이 전압문제는 opto-coupler를 매개로 해결할 수 있다. 전압 분배를 위해 코어리스 트랜스포머를 포함했고 드라이버에 사용된 이 트랜스포머는 1,700V까지 감당할 수 있으며 데이터 전송은 100V/ns의 slew rate를 보인다.

제안된 드라이버 IC에서 트랜스미터와 리시버, 파워 레귤레이션, 레퍼런스와 컨트롤, 그리고 두 개의 게이트 드라이버가 메인 부분이다. Switched mode power supplies(SMPS)를 위한 고전력, 고효율 시스템을 소개했으며 Switch와 Driver 및 Powering System을 보였다. 그리고 SMPS 기반의 SiC-JFET이 효율 99%에서 10kW 이상의 전력을 수용할 수 있음을 알 수 있었다.

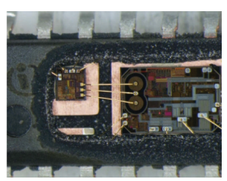


Fig5. Photograph of an opened driver IC

이번 학술대회에서는 새로운 기술과 설계기법이 도입되어 다양한 성과를 내고 있음을 알 수 있었다. 흔히 IT는 미주지역과 아시아에서 강세를 보이고 있는 것으로 생각되는데, 유럽 각국에서 온 산업계, 학계 관계자들을 보며 유럽도 아직까지 전통적 전자시장에서는 활발하게 연구를 수행하고 있다는 것을 새삼 느낄 수 있었다. 아울러 국내에는 대학원생들의 상당 부분이 유학생으로 채워지고 있는 현실에서 유럽은 자국민들의 인력을 안정적으로 확보한 것을 알 수 있었다.

경북대학교 전자공학부
경북대 모바일 – AP 플랫폼 센터 CEO
최준림 교수
연구분야 : System On Chip, 마이크로 센서, 디지털 시스템 설계
E-mail : jrchoi@ee.knu.ac.kr
http://digital.knu.ac.kr

SPECIAL Column II

Active-HDL

A. 목적 : FPGA Design & Simulation

B. 구분 : Aldec 사의 Active-HDL 툴은 FPGA design과 시뮬레이션솔루션 관련 설계 플로우 관리자를 통합 제공.

C. Supported platform and O/S System
- Windows 7
- Vista/XP/2003 32/64 bit support

D. 특성 및 기능

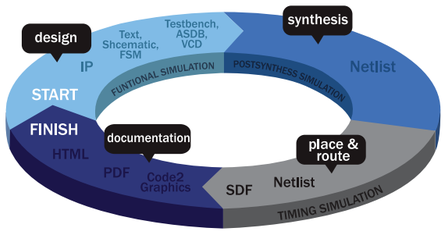
Active-HDL은 FPGA용 디자인 Simulator로서, VHDL, Verilog, SystemC 그리고 EDIF, C/C++와 SystemVerilog format을 지원합니다. Active-HDL은 VHDL, Verilog, EDIF(netlist), 또는 Mixed-HDL(VHDL and Verilog and EDIF)을 Single Kernel에서 시뮬레이션할 수 있습니다. Optimized Direct Compile Architecture를 사용함으로써 최고의 성능과 우수한 기능(디버깅 환경)을 갖는 고성능의 HDL Simulator입니다.

또한 HDE(HDL Editor),BDE(Block Diagram Editor), FSM(Finite State Machine) 등의 Design Entry 부분과 모든 FPGA, CPLD들의 library와 interface를 제공함으로써 더욱 강력한 Design Verification 환경을 지니고 있으며, 복잡한 FPGA Flow를 Active-HDL 안에서 제어함으로써 FPGA 전 단계를 구현하여 편리한 디자인 환경을 제공합니다.

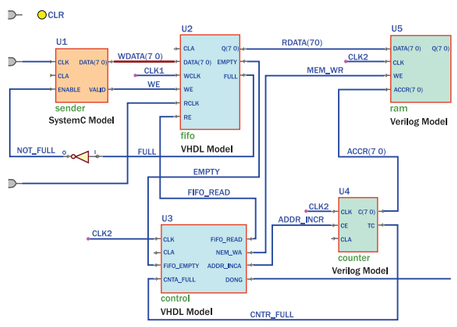
현재의 많은 FPGA 벤더들(Xilinx, Altera, Lattice, Microsemi(Actel), Quicklogic, Atmel)을 위한 시뮬레이션,

합성 구현 과정을 하나의 공통 환경에서 제어할 수 있도록 해준다. Active-HDL은 80개가 넘는 많은 EDA 툴들과의 인터페이스를 가지고 있어서 아주 강력한 플랫폼을 만들어준다.

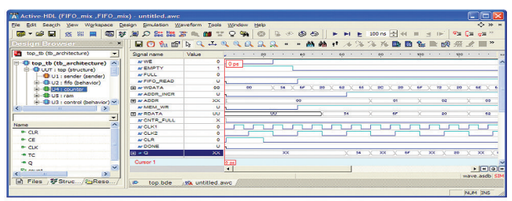
FPGA Design Flow



Graphic Design Entry : Active-HDL은 FSM 다이어그램을 그리고 이것을 합성 가능한 RTL로 만들어 주고, 내장된 블록 다이아그램 편집기를 이용해서 모든 디자인 모듈들을 Top 레벨에서 연결하고 구조적인 HDL을 생성할 수 있는 기능들을 제공한다. 필요하다면 반대로 Code2Graphics 유틸리티를 이용해서 HDL을 그래픽 형태로 바꿀 수도 있다. Active-HDL은 또한 예전의 디자인들을 불러오고, Re-target하고, 개선하고, 시뮬레이션하고, 디버그할 수 있다.



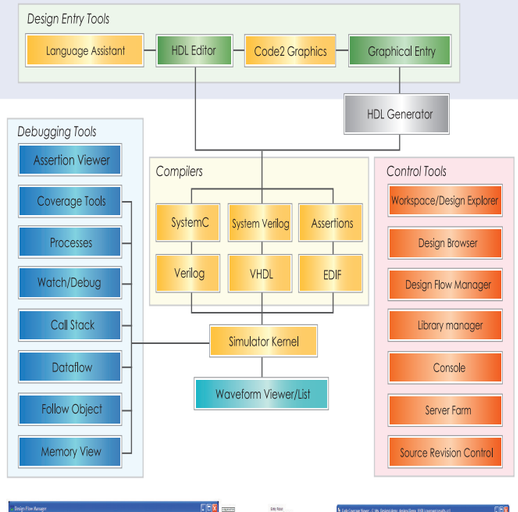
High Performance, Mixed-Language Simulation : Active-HDL은 고성능, 공통-커널, 배치모드 시뮬레이션을 지원하는 mixed-language 시뮬레이터, VCD, 성능 프로파일러, Memory Viewer, 암호화 IP 그리고 FPGA 벤더 라이브러리들을 포함한다. 복합적인 테스트벤치들을 이용해서 시스템 레벨의 시뮬레이션 모델을 드라이브하고 디자인과 시스템 레벨 디자인들을 빠르게 테스트하도록 빠르고 유연한 시뮬레이터장을 만든다.

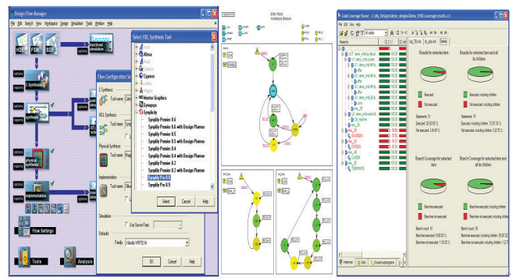


Debugging and Code Coverage : Active-HDL은 가속화된 파형, HDL 소스 코드와의 교차 점검, 브레이크포인트 관리, 테스트벤치와 테스트 입력 생성과 같은 최첨단의 디버깅 기능들을 포함한다. 강력한 Code Coverage 분석기는 디자인의 모든 문구, 라인, 신호, 토글, 브랜치, 경로, 그리고 논리적 표현들의 100% 테스트 커버리지를 제공한다.

Top Features

- Common-Kernel Mixed Language Simulator
- Languages: VHDL, Verilog®, SystemVerilog (Design, Verification & Assertions), SystemC & EDIF
- HDL Design Tools: 다양한 설계 tool을 제공 하여 편리하게 HDL 설계를 가능하게 함 – Design entry, Design Creation, Code2Graphics™, Block and State Diagram, Waveform editor, stimulus generation, Language templates & auto-complete, scripting, legacy design 지원.
- Design Flow Manager: 유저가 사용하고자 하는 FPGA tool을 하나의 통합 환경에서 등록하여 사용 가능 – FPGA 구현 시 편의성을 극대화함.
- Debugging: Code execution tracing, Waveform/Compare, Memory Viewer, Xtrace, Advanced Dataflow and Profiler.
- Coverage: Code Coverage, Toggle & Functional Coverage.
- Additional Interfaces: DSP/HDL algorithm MATLAB2® and Simulink2® Interfaces & Zuken CADSTAR PCB Design
- Assertion and Coverage (OPTION): SystemVerilog PSL & OVA 지원. Dedicated Assertion viewer, coverage, breakpoint editor.





FEATURES	PRODUCT CONFIGURATION			
	DM	Designer Edition	PE	EE
Design Entry and Doumentation				
HDL, Text, Block Diagram and State Machine Editor	·	·	·	·
Language Assistant with Templates and Auto-Complete	·	·	·	·
Macro, Tcl/Tk, Perl script Support	·	·	·	·
Mouse Strokes	·	·	·	·
Code2Grapgics™ Converter	·		·	·
Legacy Schematic Design Impore and Symbol Import/Export	·		·	·
Export to PDF/HTML/Bitmap Graphics	·		·	·
Advanced Export to PDF (Vector Graphics)	Option		·	·
Project Management				
Design Flow Manager for All FPGA Vendors	·	·	·	·
Revision Control Interface	·	·	·	·
Team-based Design Management	·	·	·	·
PCB interface	·		·	·
Code Generation Tools				
IP Core Component Generator	·		·	·
Testbench Generation from Waveforms			·	·
Testbench Generation from State Diagram			·	·
Supported Standards				
VHDL IEEE 1076 (1987, 1993, 2002 and 2008)	·	·	·	·
Verilog® HDL IEEE 1364 (1995, 2001 and 2005)	·	·	·	·
SystemVerilog IEEE 1800™ 2009 (Design)	·	·	·	·
EDIF 2 0 0			·	·
SystemC™ 2.2 IEEE 1666™ /OSCI 2.2/TLM 2.0			Option	·
Simulation/Verification				
Simulation Performance (Baseline 2X Faster than FPGA Vendor Supplied Simulator)		Baseline	3X Baseline	Up to ∞ Baseline
Single or Mixed Language Design Support	Mixed Only	Mixed Only	·	·
Simulation Model Protection/Library Encryption		·	·	·
VHDL/Verilog IEEE Compatible Encryption		·	·	·
Value Change Dump (VCD and Extended VCD) Support		·	·	·
Verilog Programming Language Interface(PLI/VPI)		·	·	·
VHDL Programming Language Interface (VHPI)			·	·
Batch Mode Simulation/Regression (VSimSA)			·	·
Pre-compiled FPGA Vendor Libraies	·	·	·	·
Xilinx Secure IP Support		·	·	·
Altera® Language-Neutral Libraries		·	·	·
Microsemi Language-Neutral Libraries		·	·	·
Profiler (Performance Metrics)			Option	·
SFM (Server Farm Manager)			Option	Option
HDL Debug and Analysis				
Interactive Code Execution Tracing		·	·	·
Advanced Breakpoint Management		·	·	·
Memory Viewer		·	·	·
Waveform Viewer		·	·	·
Waveform Stimulator			·	·
Waveform Comparison and Editing			·	·
Post-Simulation Debug			·	·
C++ Debugger			·	·
Signal Agent (VHDL and Mixed Only)			·	·
X-Trace			·	·
Advanced Dataflow			·	·
Integration with Riviera-PRO and ALINT	Option		Option	·
Assertions Debugging			Option	Option
Assertions and Coverage Tools				
Code, Statement, Branch, Expression, Condition and Toggle Coverage			·	·
PSL IEEE 1850, Systemverilog IEEE 1800™, OpenVera Assertions			Option	Option
Design Rule Checking				
ALINT™ with Aldec Basic Rule Library			Option	·
DO-254 VHDL or Verilog Rule Library			Option	Option
STARC® VHDL or Verilog Rule Library			Option	Option
RMM verilog and VHDL Rule Linrary			Option	Option
Co-Simulation				
Simulink® Co-Simulation			·	·
MATLAB® Co-Simulation			Option	·
Supported Platforms				
Windows® 7/Vista/XP/2003 32/64 bit	·	·	·	·

S.Korea

SoAR Solution, Inc

회사명 : (주)소어솔류션
웹주소 : www.aldec.com 전화 : 031-717-3560
E-mail : ybcho@soarsolution.com
주소 : 경기도 분당시 수내동 16-3