
반도체설계교육센터
IC DESIGN EDUCATION CENTER
305-701 대전광역시 유성구 대학로 291


# IDEC Newsletter


IDEC Newsletter | 통권 : 제183호 발행일 | 2012년 8월 31일 발행인 | 박[illegible] | 김이섭 제 작 | 푸울디자인
기 획 | 전향기 전 화 | 042) 350-8535 팩 스 | 042) 350-8540 홈페[illegible] | http://idec.or.kr
E-mail | jhg0929@idec.or.kr 발행처 | 반도체설계교육센터(IDEC)

Vol.183

2012 September





반도체설계교육센터 사업은 지식경제부, 반도체산업협회, 반도체회사(삼성전자, 하이닉스반도체, 매그나칩반도체, 동부하이텍, 앰코테크놀로지코리아, KEC, 세미텍, TowerJazz)의 지원으로 수행되고 있습니다.


## 보안시스템에 대한 차분 전력 분석(Differential Power Analysis, DPA) 공격과 이에 대응하기 위한 회로 설계 기법

최근 보안용 소자는 통신, 금융 및 행정 서비스 등의 광범위한 영역에서, 스마트카드 및 전자여권 등과 같이 휴대가 용이한 보안 장치의 형태로 구현되어 사용되고 있다. 이와 같은 보안 장치에는 사용자의 개인 정보와 같은 고도의 보안이 요구되는 정보가 저장되어 사용되고 있으며, 언제 어디서나 쉽게 이용할 수 있는 장점이 있는 반면, 탈취에 의한 물리 공격 및 복제에 의한 공격으로부터 취약할 수 있다 본고에서는 강력한 공격 방법인 DPA에 대하여 살펴본 후, 이에 대응하기 위하여 셀 레벨 에서 사용되는 dual-rail precharge(DRP) 논리회로와 그 적용 예를 소개한 후, 이의 단점을 보완한 symmetric adiabatic logic circuit (SyAL)에 대해서 설명함으로써 DPA 공격을 어떻게 효과적으로 방어할 수 있는지 알아보도록 한다. (관련기사 P04~09 참조)

## 차량 인식 기술 소개

무인 운전 또는 자동 운전은 더는 꿈이나 공상과학 얘기가 아니다. 지난 2012년 5월에 미국 네바다 주에서 구글 무인 운전 자동차가 테스트에 통과하여, 무인 운전 자동차 운전 면허증을 발급받았다. 현재, 스마트 차량의 실용화를 위한 많은 연구가 진행중이다. 도로 위의 다른 차량, 보행자, 건물 등을 인식하기 위해서, 수동적인 센서인 카메라에서부터 능동적인 센서인 레이저까지 다양한 각도에서 접근하고 있다. 그러나 능동적 센서가 다른 기기에 비해 상대적으로 고가이며 가까운 거리를 측정할 수 없는 등의 단점들을 가지고 있다. 본 고에서는 수동적 센서인 차량용 카메라를 이용한 영상 비전으로 개발된 다양한 차량 인식 기술을 소개하기로 한다. (관련기사 P10~12 참조)

## 모바일 기기의 융합시대 : 모바일-AP IDEC 플랫폼 센터 (IPC)

모바일 기기가 모바일 인터넷 대중화 시대를 열고 있다. "스마트폰으로 하루를 시작하여 스마트폰으로 마감한다."는 소비층이 등장할 정도로 스마트폰 및 모바일 기기의 영향력이 커지고 있다. 2011년 스마트폰 보급 대수는 약 7.3억대, 스마트폰을 제외한 모바일 기기는 약 3.6억대로 Gartner 조사를 바탕으로 예측한 2015년 전체 모바일 기기는 37억대, 2020년에는 100억대로 늘어날 전망이다. 본 고에서는 경북대 모바일-AP 플래폼 센터의 소개 및 포부를 최준림 CEO를 통해 들어보고자 한다. (관련기사 P14~P17 참조)

## IEEE ISCAS 2012 최초 한국 개최를 무사히 마치고

1968년 미국 마이애미를 시작으로 매년 개최되는 ISCAS 국제학술회의는 1963년 설립된 국제전기전자 학회인 IEEE(Institute of Electrical and Electronics Engineers) 주관 국제학술대회 중 가장 역사가 긴 학술대회이다. 또한, IEEE CASS에서 주관하는 IT, 반도체 및 응용분야의 국제학술회의로 세계 최대 규모이다. 본 고에서는 최초 한국에서 개최한 IEEE ISCAS 2012의 모습을 아주대학교 선우명훈의 시선으로 살펴보고자 한다.
(관련기사 P18~P19 참조)

# IDEC news

September | 2012

## MPW (Multi-Project Wafer)

### MPW 신청 현황 |

| 구분 | 공정 | 제작가능 면적 (mm²x 칩수) | 채택 팀수 | 설계면적 (mm² x 칩수) | DB마감 | Die-out | 비고 |
|---|---|---|---|---|---|---|---|
| 114회 (12-7) | M/H 0.18 | 4.5x4㎟x20 | 20 | 4.5x4㎟x20 | 2012. 8.13 | 2012. 12.3 | DB 검토중 |
| | 삼성 0.13 | 4x4㎟x48 | 34 | 4x4㎟x34 | 2012. 8.31 | 2013. 1.4 | DB 접수중 |
| 115회 (12-8) | 동부 0.18BCD | 5x5㎟x2 | 5 | 5x2.5㎟x3 2.5x2.5㎟x2 | 2012. 9.6 | 2013. 1.4 | 모집마감 |
| | TJ0.18 CIS | 2.5x2.5㎟x4 | 4 | 2.5x2.5㎟x4 | 2012. 10.15 | 2013. 2.22 | 모집마감 |
| | TJ0.18 BCD | 5x5㎟x2 | 1 | 5x5㎟x1 | 2012. 10.22 | 2013. 2.29 | 모집중 |
| 116회 (12-9) | TJ0.18 RF | 2.5x2.5㎟x4 | 3 | 2.5x2.5㎟x3 | 2012. 10.22 | 2013. 2.29 | |
| | 동부 0.35BCD | 5x2.5㎟x6 | 8 | 5x2.5㎟x4 2.5x2.5㎟x4 | 2012. 10.10 | 2013. 1.16 | 모집마감 |
| | 동부 0.11 | 5x2.5㎟x30 | 33 | 5x2.5㎟x27 2.5x2.5㎟x6 | 2012. 10.2 | 2013. 2.6 | |
| 117회 (12-10) | M/H 0.18 | 4.5x4㎟x20 | 20 | 4.5x4㎟x20 | 2012. 11.12 | 2013. 3.4 | 모집마감 |
| | M/H 0.35 | 5x4㎟x20 | 20 | 5x4㎟x20 | 2012. 11.12 | 2013. 3.4 | |
| | 삼성 65nm | 20개서버 (4x4㎟) | 17 (서버) | 4x4㎟x18 | 2012. 11.26 | 2013. 5.3 | |

* 2012년 MPW 모집이 완료됨. 2013년 MPW 지원 공정 및 일정은 2012. 11월 이후 공지 예정

### MPW 칩 제작 현황 |

| 구분 | 공정 | 제작 칩수 | 제작면적 (mm²x칩수) | Die-out 예정일 | 현재상태 | 비고 |
|---|---|---|---|---|---|---|
| 108회 (12-1) | M/H 0.18 | 20 | 4.5x4㎟ x 20 | 2012. 6.4 | PKG 제작중 | -Die:7.21 -PKG:8.24 |
| | 동부 0.35BCD | 16 | 5x2.5㎟ x 2 2.5x2.5㎟ x 8 | 2012. 5.30 | 제작완료 | -Die: 5.15 -PKG:6.10 |
| | TJ0.18 SiGe | 4 | 2.5x2.5㎟ x 4 | 2012. 7.2 | 제작완료 | -Die:7.19 |
| | TJ0.18 RF | 8 | 2.5x2.5㎟ x 4 | 2012. 7.5 | 제작완료 | -Die:6.18 |
| 109회 (12-2) | 삼성 0.13 | 40 | 4x4㎟ x 40 | 2012. 8.3 | PKG 제작중 | -Die:8.17 -PKG:9.10예정 |
| 110회 (12-3) | 동부 0.35BCD | 9 | 5x2.5㎟ x 2 2.5x2.5㎟ x 7 | 2012. 7.12 | 제작완료 | -Die:7.10 |
| | 동부 0.11 | 29 | 5x2.5㎟ x 22 2.5x2.5㎟ x 7 | 2012. 8.1 | 제작중 | Fab out: 8.24예정 |
| 111회 (12-4) | M/H 0.18 | 20 | 4.5x4㎟x20 | 2012. 9.3 | 제작중 | |
| | M/H 0.35 | 20 | 5x4㎟x20 | 2012. 9.3 | 제작중 | |
| | 동부 0.35BCD | 7 | 5x2.5㎟x4 2.5x2.5㎟x3 | 2012. 8.30 | 제작중 | |
| | TJ0.18 CIS | 2 | 5x2.5㎟x2 | 2012. 9.14 | 제작중 | |
| | TJ0.18 BCD | 2 | 5x5㎟x2 | 2012. 9.21 | 제작중 | |
| 112회 (12-5) | 삼성 65nm | 23 | 5x5㎟x23 | 2012. 11.9 | 제작중 | |
| | 동부 0.18BCD | 4 | 5x2.5㎟x4 | 2012. 9.26 | 제작중 | |
| 113회 (12-6) | 동부 0.35BCD | 9 | 5x2.5㎟x4 2.5x2.5㎟x4 | 2012. 10.10 | 제작중 | |

* M/H = 매그나칩/하이닉스, TJ = TowerJazz
* 우선/정규모집에서 마감될 경우 후기모집은 진행되지 않음.
* Die-out 일정은 Diechip 제작완료 기준임. Package는 Die-out후 4주 이상 소요됨.
* MPW 참여 일정 및 방법은 홈페이지(www.idec.or.kr) 참조
* 위의 내용은 8.24 기준임.

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

## 2013년 WG 선정 안내

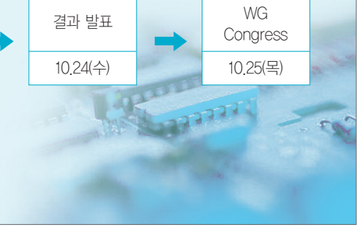
시스템반도체 설계인력 양성과 핵심적인 IP 개발을 위하여 IDEC에서는 2013년 WG(working group)을 선정하여 지원하고자 한다.
WG 선정 기준은 기존참여교수는 당해연도 활동실적과 차년도 계획, 신규참여교수는 차년도 계획으로 진행되면 선정절차는 아래와 같다.

• **선정 절차**

| WG 선정안내 | → | 지원신청서 제출 마감 | → | 실적결과 조회 및 수정 | → | 서류심사 | → | 결과 발표 | → | WG Congress |
|---|---|---|---|---|---|---|---|---|---|---|
| 8.31(금) | | 10.05(금) | | 10.9 ~10.11 | | 10.15~10.22 | | 10.24(수) | | 10.25(목) |

• **지원신청서 작성 :** IDEC 홈페이지 (http://idec.or.kr) 참고

• **문의 :** 김은주(042-350-8533, ejkim@idec.or.kr)



## 2012년 9월 교육프로그램 안내

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

### 강좌 일정 |

| 강의일자 | 강의제목 | 분류 |
|---|---|---|
| 9월 4일-6일 | Design Compiler 사용법 및 활용예 | Tool강좌 |
| 9월 11일-12일 | Core-A 프로세서를 활용한 영상 입출력 플랫폼 설계와 검증 | 설계강좌 |
| 9월 18일-20일 | PrimeTime 사용법 및 활용예 | Tool강좌 |
| 9월 25일-27일 | IC Compiler 사용법 및 활용예 | Tool강좌 |

### ▷본센터 강좌 일정

■ 강좌일 : 9월 4일-6일
■ 강좌 제목 : Design Compiler 사용법 및 활용예
■ 강사 : 박동원(파인스)

**[ 강좌개요 ]**
Synopsys의 Design Compiler를 사용하여 VHDL 또는 VerilogHDL로 구성된 RTL Netlist를 Gate Level Netlist로 변환하고 각각의 작업 단계에 따른 적절한 설계기법과 환경 등을 살펴본다.

**[ 수강대상 ]**
· Design Compiler 사용자

**[ 강의수준 ]** · 초급
**[강의형태]** · 이론+실습

■ 강좌일 : 9월 11일-12일
■ 강좌 제목 : Core-A 프로세서를 활용한 영상 입출력 플랫폼 설계와 검증
■ 강사 : 기안도 소장(다이나릿시스템)

**[ 강좌개요 ]**
프로세서를 활용한 시스템을 설계하는 방법을 소개하고, Core-A 프로세서를 활용한 플랫폼을 설계하고, 영상 입출력에 필요한 LCD 제어기와 카메라 제어기를 설계하여 프랫폼에 적용하여 영상입출력 플랫폼을 설계한다. 설계과정에서는 RTL 시뮬레이션, HW/SW 통합시뮬에이션, 로직 합성, FPGA 프로토타이핑 등 플랫폼 설계 과정을 실습한다. 이를 통해 프로세싱 코어를 활용한 하드웨어/소프트웨어 통합 시스템 설계에 대한 방법을 배우고 실습하고, 영상정보를 처리하는 플랫폼을 구현하여 이미지 처리 시스템에 대해 배운다.

**[ 수강대상 ]**
· 내장형 시스템 설계자, 영상 입력 시스템 설계자, 영상 출력 시스템 설계자

**[ 강의수준 ]**
· 중고급
**[강의형태]** · 이론+실습

**[ 사전지식,선수과목 ]**
· 디지털 로직; 컴퓨터 구조; Verilog-HDL; C; 마이크로 프로세서; HDL simulation; Logic synthesis; FPGA, Core-A

■ 강좌일 : 강좌일 : 9월 18일-20일
■ 강좌 제목 : PrimeTime 사용법 및 활용예
■ 강사 : 한동환(파인스)

**[ 강좌개요 ]**
Synthesis 후 Timing 분석을 위해 Synopsys 사의 PrimeTime 이란 Satic Timing Analysis Tool을 효율적으로 사용하는 법을 익힌다.

**[ 수강대상 ]**
· PrimeTime 사용자

**[ 강의수준 ]** · 초급
**[강의형태]** · 이론+실습

**[ 사전지식,선수과목 ]**
· Design Compiler

■ 강좌일 : 9월 25일-27일
■ 강좌 제목 : IC Compiler 사용법 및 활용예
■ 강사 : 양용규(파인스)

**[ 강좌개요 ]**
Synopsys의 auto place & routing tool인 IC compiler 의 기초를 이해하고, 필요한 input file 및 각 단계별 key command를 강의를 통하여 습득한 후 sample design에 대해 IC compiler를 직접 실행하여 real physical design에 적용할 수 있는 능력을 배양하고자 함

**[ 수강대상 ]**
· IC Compiler 사용자

**[ 강의수준 ]** · 초급
**[강의형태]** · 이론+실습

**[ 사전지식,선수과목 ]**
· 1) Design Compiler 2) PrimeTime

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

## Chip Design Contest(CDC)

### • International SoC Design Conference(ISOCC) 2012 Chip Design Contest 개최

** Chip Design Contest(CDC)는 ISOCC 2012프로그램의 한세션으로 진행되나 논문은 프로시딩(Proceedings)에는 포함되지 않음.

**1. 일정 및 장소**
가. 진행 일정 : 2012년 11월 5일(월)
나. 장 소 : 제주 라마다 호텔
다. CDC 주요 일정

| 논문 제출 마감 | 논문 채택 통보 | Chip Design Contest |
|---|---|---|
| 2012. 8. 25 | 2012. 10. 1 | 2012. 11. 5 |

* 일정은 사정에 따라 다소 변경될 수 있습니다.

**2. 논문 접수 분야 :** SoC 설계

**3. 시상내역**

| 시 상 명 | | | 내 역 |
|---|---|---|---|
| Best Design Award | 일반부문 | 최우수상(1팀) | 상장 및 상금 100만원 |
| | | 우수상(2팀) | 각 상장 및 상금 50만원 |
| | 특별상부문 | SSCS 서울챕터상(1팀) | 상장 및 상금 50만원 |

* 수상팀수는 사정에 따라 변경될 수 있습니다.

### • 제20회 한국반도체학술대회 Chip Design Contest 개최

**1. 일정 및 장소**
가. 진행 일정 : 2013년 2월 5일(화)
나. 장 소 : 횡성 성우리조트
다. CDC 주요 일정

| 논문 제출 마감 | 논문 채택 통보 | Chip Design Contest |
|---|---|---|
| 2012. 10. 19 | 2012. 12. 1 | 2013. 2. 5 |

* 일정은 사정에 따라 다소 변경될 수 있습니다.

**2. 논문 접수 분야 :** SoC 설계

**3. 시상내역 :** ISOCC CDC와 동일함.

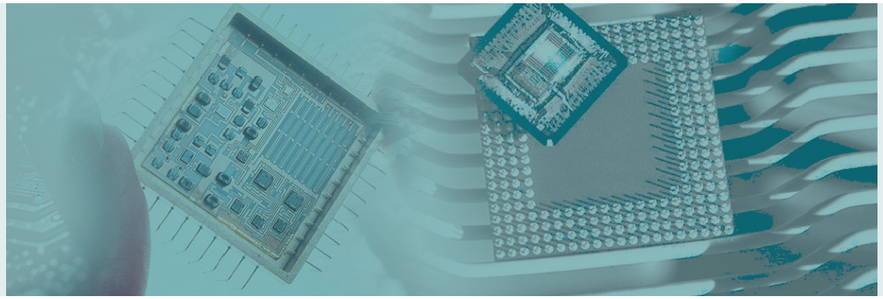
* CDC 참여와 관련한 자세한 사항은 홈페이지 (http://idec.or.kr)를 참고해 주시기 바랍니다.

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

# 보안시스템에 대한 차분 전력 분석 (Differential Power Analysis, DPA) 공격과 이에 대응하기 위한 회로 설계 기법

한양대학교 융합전자공학부
최병덕 교수
연구분야 : Analog and mixed-signal IC, PMIC Driving methods and circuits for FPD, Hardware implementation of cyrptographic devices, Low-power and low-noise IC for biomedical applications
E-mail : bdchoi@hanyang.ac.kr
http://delab.hanyang.ac.kr

한양대학교 전자컴퓨터통신공학과
전두현 석박통합과정
연구분야 : Analog circuit design Display driving circuit design, Hardware implementation of cyrptographic devices
E-mail: dhjeon@hanyang.ac.kr
http://delab.hanyang.ac.kr



## 서론

최근 보안용 소자는 통신, 금융 및 행정 서비스 등의 광범위한 영역에서, 스마트카드 및 전자여권 등과 같이 휴대가 용이한 보안 장치의 형태로 구현되어 사용되고 있다. 이와 같은 보안 장치에는 사용자의 개인 정보와 같은 고도의 보안이 요구되는 정보가 저장되어 사용되고 있으며, 언제 어디서나 쉽게 이용할 수 있는 장점이 있는 반면, 탈취에 의한 물리 공격 및 복제에 의한 공격으로부터 취약할 수 있다.

특히 부채널 공격(side channel attack, SCA)은, 값비싼 장비를 이용해야 하는 공격과 달리 비교적 적은 비용과 노력으로도 간단히 보안용 소자의 정보를 파악할 수 있기 때문에 이로부터 보안 장치를 안전하게 보호하는 것은 매우 중요하다.

부채널 공격이란 보안용 소자에 물리적 손상을 주지 않고, 암호화 알고리즘이 동작하는 동안 부가적으로 발생하는 정보, 즉, 연산 시간, 소비 전력, 전자파 등의 정보(이를 부채널 정보라 함)를 이용하는 공격방법으로, 보안용 소자의 정상적인 동작을 유지하면서 공격이 가능하다. 그 중에서도 전력 분석 방법 중에 하나인 차분전력분석(differential power analysis, DPA) 공격은 그 공격방법이 상대적으로 쉬우면서도 매우 강력한 공격능력을 가지고 있기 때문에 많이 사용하고 있는 공격 방법이다.[1]

따라서 보안용 소자가 DPA 공격을 방어할 수 있는 기능을 갖는 것은 필수적이라고 할 수 있으며, 이에 다양한 대응방법이 제시되어 왔다. 크게 아키텍처 레벨과 셀 레벨로 분류할 수 있는데, 아키텍처의 접근 방식은, 기존의 스탠다드 셀과 그 설계 기법을 그대로 사용할 수 있다는 장점이 있는 반면, 셀 레벨 접근 방식은 전력소모와 직접적으로 연관되는 디지털 로직의 셀 단위에서 방어가 이루어지기 때문에 전자에 비해 보다 근본적으로 방어할 수 있는 장점이 있다.

본고에서는 강력한 공격 방법인 DPA에 대하여 살펴본 후, 이에 대응하기 위하여 셀 레벨 에서 사용되는 dual-rail precharge(DRP) 논리회로와 그 적용 예를 소개한 후, 이의 단점을 보완한 symmetric adiabatic logic circuit (SyAL)에 대해서 설명함으로써 DPA 공격을 어떻게 효과적으로 방어할 수 있는지 알아보도록 한다.

## 본론

### ■ 부채널 공격(side channel attack, SCA)의 개념

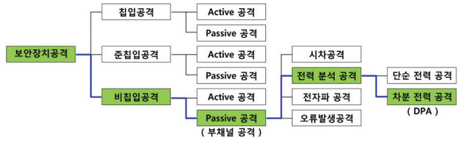



그림 1. 보안 장치 공격 방법

보안 장치를 공격하는 방법은 그 기준에 따라 다양하게 분류되는데 이에 대한 분류를 그림 1에 나타내었다. 공격하는 인터페이스에 따라 침입공격, 준 침입공격, 및 비 침입공격으로 분류할 수 있고, 공격하는 방식에 따라 active 공격과 passive 공격이 있다. 특히, passive 방식의 비 침입공격은 보안 장치를 파괴하지 않고, 정상적인 동작을 그대로 유지한 상태에서 수행한다. 암호화 알고리즘이 동작하는 동안 공격자는 내부 구조의 상세한 정보는 알 수 없지만, 알고리즘이 연산되는 시간이 어떻게 되는지, 장치의 입력에 따라 소비되는 전력 또는 발생하는 전자파가 어떻게 달라지는지를 살펴봄으로써 알고리즘의 보안 공격이 가능하게 된다. 이러한 공격 방법을 부채널 공격(side channel attack, SCA)이라고 하며, 시차 공격, 전력 분석 공격, 전자파 분석, 오류 발생공격 등이 있다.

### ■ 전력 분석 공격(power analysis)

부 채널 공격 방법 중에서도 가장 대표적인 공격방법이 전력 분석 공격이다. 전력 분석 공격은 디지털 로직으로 구성된 하드웨어 내부의 '0', '1'의 값이 변화는 모습에 따라 소모되는 전력의 양상이 다르다는 점을 이용하는 공격 방법으로, 암호 키를 처리하는 시간 동안의 전력을 분석하여 암호 키 및 보안정보를 얻어내는 방법이다. 디지털 로직 값에 따라 어떻게 소비전력이 달라지는지는, 기본적인 논리회로 중 하나인 그림 2의 인버터 동작을 통해 쉽게 설명할 수 있다.

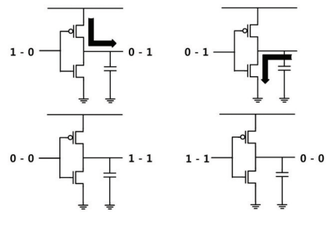



그림 2. 인버터 입력 값에 따른 전류의 흐름.

인버터 의 입력이 '1'에서 '0'으로 변하는 동작에서는 출력 값이 '0'에서 '1'로 "충전" 하는 동작을 하는 반면, 입력이 '0'에서 '1'로 변하는 동작에서는 "방전"하는 동작을 한다. 입력 값이 '0'에서 '0' 또는 '1'에서 '1'로 변하지 않고 유지되는 조건에서는 별도의 충방전 동작이 일어나지 않는다. 이는 입력 값에 따라서 인버터가 전류를 소비하는 형태가 다르기 때문에, 역으로 전력분석을 통해 현재 입력으로 어떠한 값이 사용되고 있는지 유추해 낼 수 있다.

이와 같은 원리를 이용한 공격 방법을 전력 분석(power analysis) 방법이라 하고, 전력 패턴을 분석하는 방법에 따라 단순 전력 분석(Simple Power Analysis, SPA)과 차분 전력 분석(Differential Power Analysis, DPA)로 구분된다. 단순 전력 분석은 공격자가 내부 암호화 알고리즘을 알고 있을 때 취할 수 있는 공격 방법으로, 시간 축에 따른 소비 전력의 패턴을 보고 공격하려는 암호화 알고리즘이 어떻게 구성되어 있는지 알아내는 공격 방법이다.

반면 차분 전력 분석은 시간 축에 따른 소비전력의 패턴 뿐만이 아니라, 입력 데이터와 소비전력간의 상관관계도 함께 분석하는 방법을 사용한다.[1] 이러한 상관관계를 이용한 방법은 SPA 보다도 더욱 효과적으로 보안용 소자를 공격할 수 있게 한다.

### ■ 차분 전력 분석(differential power analysis, DPA)

앞에서 언급한 바와 같이 DPA 공격은 시간에 따른 암호화 알고리즘의 전력 소모 패턴을 분석할 뿐만 아니라 입력 데이터 와 알고리즘의 소모 전력의 상관 관계를 함께 분석하는 방법을 함께 사용한다.

이러한 방법은 암호화 알고리즘이 어떻게 구성되어 있고, 입력 값에 따라 어떠한 패턴으로 전력이 소비되는지에 대한 정보를 공격자가 알지 못하더라도, 알고리즘의 입력 데이터와 소비 전력의 상관 관계로부터 예측하는 암호 키의 일치 여부를 판단할 수 있다. 이는 단순히 공격자가 암호화 알고리즘을 동작시킬 수 있는 정보만 있다면 공격이 가능하게 하므로 비교적 쉬운 공격방법을 사용하여 신뢰할 수 있는 정보를 얻을 수 있다.

따라서 보안용 소자에 DPA 공격에 대응하는 방법을 구비하는 것은 필수적이라고 할 수 있으며, 기본적으로 알고리즘에 사용되는 데이터와 소비전력의 상관관계를 제거할 필요가 있다.

### ■ DPA의 대응방법

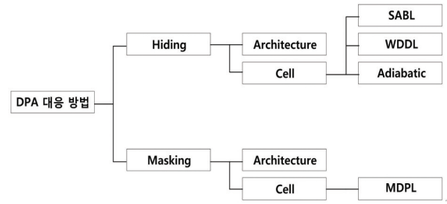



그림 3. DPA 공격의 대응 방법 분류

암호화 알고리즘에서 사용하는 암호화 키와 전력 소모의 연관성을 제거하기 위한 방법은 크게 hiding과 masking 두 가지로 분류할 수 있다. Hiding 방법은 암호화 알고리즘에서 사용되는 보안용 소자의 데이터 값과 소비전력의 상관 관계가 없도록 만들기 위해서 데이터 값과 무관하게 일정하거나 랜덤한 소비 전력이 발생하도록 하여 DPA에 대응한다.

반면 masking 방법은 소비 전력에 영향을 주는 보안용 소자의 데이터 값을 암호화 정보가 담겨있지 않는 랜덤한 값으로 바꾸는 방법으로, 보안용 소자의 데이터와 소비 전력에는 서로 상관관계를 가지고 있더라도, 데이터에는 암호화 정보가 무관한 랜덤 값이 들어있기 때문에 DPA공격으로부터 방어할 수 있다. 이 두 종류 대응방법이 셀 레벨에서 어떻게 DPA 공격에 대응할 수 있는지 살펴 본다.

### ■ Hiding을 이용한 DPA 대응 방법

#### ■ Hiding 개요

Hiding 이란 보안용 소자의 소비 전력이 입력 데이터와는 무관하도록 만드는 방법으로, 소비되는 전력을 입력 값과 상관없이 랜덤하거나 일정하게 한다. 셀 레벨에서는 주로 상보 논리 회로를 구성하여 대칭 구조를 사용하며, 입력 값이 다르더라도 일정한 전력을 소모하게 한다.

소비 전력을 일정하게 하기 위한 구조로 dual-rail precharge (DRP) 논리회로가 주로 사용된다. DRP 논리회로란, 입력이 '0' 또는 '1'인 차이로부터 발생하는 소비전력의 차이를 제거하기 위해서 입출력이 모두 '0', '1' 신호가 함께 상보적으로 구성 되어있는 dual-rail(DR) 논리회로를 사용하면서, 매 클럭마다 내부 노드를 동

일한 상태로 만들어 주기 위한 precharge 논리회로를 함께 구현한 것을 DRP 논리회로라고 한다.

DRP 논리회로 구현 시 전력을 일정하게 만들기 위해 고려해야 할 것 중 하나는 상보 신호에 대해서 동일한 커패시턴스 값을 갖도록 설계되어야 한다는 점이다. 로직 게이트의 출력 노드 뿐만 아니라 신호선의 커패시턴스 값은 소비 전력을 결정하는데 직접적으로 관여하는 요소 중 하나로, 동일한 값을 갖는 설계가 필요하다. 이를 차동 배선(differential routing)이라고 하며, precharge 이후 evaluation 구간에서 논리회로 동작 시 양쪽의 상호신호 출력 노드에 동일한 전류 경로를 갖도록 설계해야 동일 전력 소모를 기대할 수 있다.[2]

DRP 논리회로를 이용한 대표적인 구조인 Sense Amplifier Based Logic(SABL)과 Wave Dynamic Differential Logic(WDDL) 대해서 각각 살펴본다.

### ■ Sense Amplifier Based Logic(SABL)

Sense Amplifier Based Logic은 모든 셀에 클럭 신호가 연결되어 precharge를 할 수 있게 구성되어 있다.[3]

SABL의 동작을 살펴보면 다음과 같다. precharge시에 모든 입력값을 '0'으로 인가하여 두 개의 출력 값을 모두 '1'로 precharge해준다. 이 후 evaluation구간에서 입력을 상보신호로 인가해주면, 두 출력 값 중 하나의 출력 값만이 '0'으로 evaluation 되고, 다음 precharge 구간에서는 '0'으로 evaluation 된 출력 값 만이 '1'로 precharge 된다. 따라서 두 상보 출력의 값이 변화하는 패턴을 살펴보면 '1' – '0' – '1' 혹은 '1' – '1' – '1'의 모습으로 입력 데이터 값에 상관없이 앞의 두 모습으로 일정한 전류 패턴을 갖는다.

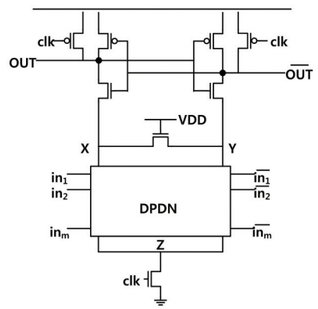



그림 4. Sense Amplifier Based Logic 셀의 회로도

그림 4는 SABL의 일반적인 회로도의 구조를 나타내며, 입력에 따른 논리회로의 동작 수행을 differential pull-down network(DPDN)이라 한다. Precharge에서는 X, Y 노드에 동시에 충전하므로 동작 시마다 동일한 전류 소모를 기대할 수 있지만, DPDN의 경우에는 입력 값에 따라 동작이 달라지게 되므로, 방전할 때의 전류 소모 패턴에 차이가 있다는 한계가 있다.

### ■ Wave Dynamic Differential Logic(WDDL)

Wave Dynamic Differential Logic은 SABL과 달리 스탠다드 셀 라이브러리에서 제공하는 single rail 셀을 이용하여 구성되며, 보다 단순한 구조를 갖는다.[4] WDDL은 순차 논리(Sequential logic) 셀만이 클럭 신호에 연결되어 이 셀들만 클럭 신호에 따라 precharge 및 evaluation 동작을 수행한다. 조합 논리(combinational logic) 셀은 입력이 precharge 값일 때 precharge되고, 상보 값 일 때 evaluation 동작을 수행한다.

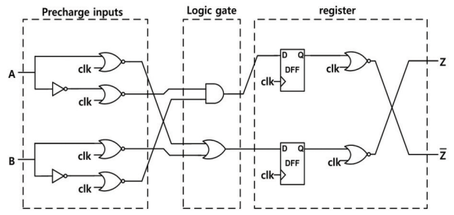



그림 5. Wave Differential Dynamic Logic AND/NAND Cell의 회로도

그림 5에 는 WDDL AND/NAND 셀의 구조를 AND-OR 게이트를 이용하여 나타내었다. 클럭이 '1'에서 precharge 구간이 되며, 모든 게이트의 출력이 '0'으로 precharge된다. 클럭이 '0'으로 변하면서 evaluation 구간으로 변하고, WDDL 셀의 논리 게이트 및 레지스터는 상보 출력 값을 갖는다.

WDDL 셀은 DPA에 대응하기 위한 구조이지만 상보 출력에 대해서 전류 소모가 완전히 동일하다고 볼 수 없는데 그 이유는 다음과 같다. 첫 번째로 논리회로 내부 노드의 충/방전 경로가 모든 입력 값에 대해서 동일하지 않다. 입력 값에 따라서 전류 경로가 달라지므로, 소모되는 전력이 입력 값에 따라 달라진다. 두 번째로 모든 내부 노드가 매 주기마다 동시에 충/방전 되지 않아 이전 데이터에 따라 내부 노드에 전하가 저장되는 "메모리 효과"를 가져올 수 있다.

## ■ Masking을 이용한 DPA 대응방법

Masking 방법은 암호화 알고리즘에서 사용되는 중간 값을 랜덤화하여 전력 분석 공격을 하더라도 암호 데이터와의 관계의 연관성을 제거하는 방법이다. 즉, DPA 공격을 통해서 소비 전력과 알고리즘 내부 값과의 상관관계를 분석하더라도, 내부 값 자체가 암호 데이터와는 무관하기 때문에 DPA공격에 대응할 수 있다.

Masking 방법으로 중간 값을 랜덤화 하는 것은 알고리즘 레벨로 쉽게 구현할 수 있다는 장점이 있지만, unmask값과 mask의 값의 연관성을 완벽하게 없애는 것은 어렵기 때문에 셀 레벨에서의 대응방법이 중요하다고 볼 수 있다. 셀 레벨의 대응은 DRP 논리회로를 사용하여 구현하게 되는데, 앞에서 살펴본 hiding 방법에서와는 달리 중간 값과 상보 신호선에서 소모되는 전력을 동일하게 맞추는 것은 필요하지 않다.

### ■ Masked Dual-Rail Precharge Logic(MDPL)

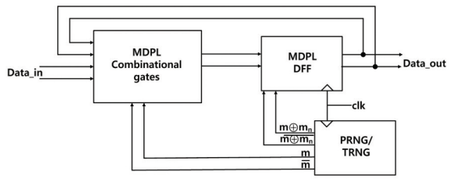



그림 6. Masked Dual-Rail Precharge Logic의 구조

MDPL은 회로의 모든 신호에 동일한 mask를 사용하여, unmask값과 XOR 연산을 수행한 mask 값이 암호화 알고리즘 연산에 사용된다.[5] 그 구조는 hiding의 WDDL과 유사한 모습을 가지며, majority(MAJ) 셀을 기본으로 구성된다.

MAJ 셀은 unmask값과 mask를 입력으로 masked 출력 값을 갖는 majority function을 연산한다. c의 논리 값에 따라서 a, b 입력에 대한 MAJ의 연산이 달라지는데, c=0에서는 AND 연산을 하고, c=1에서는 OR 연산을 한다. 일반적인 구조는 그림 6과 같다. Precharge 및 evaluation 동작이 끝나면, MDPL DFF에서는 mask 값을 교체하고 다음 클럭 주기에 사용한다. MDPL에서 사용되는 MDPL AND/NAND 게이트와 MAJ 셀을 그림 7에 나타내었다.

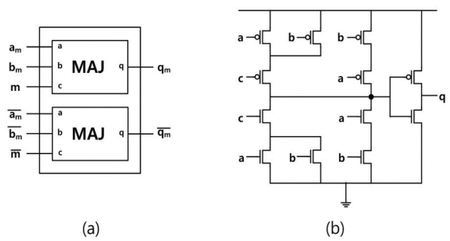



그림 7. MDPL AND/NAND
(a) 논리 게이트 회로도 및 (b) MAJ 셀 회로도

MDPL 회로는 기존 CMOS 회로에 비해 2배이상의 면적을 가지며, 최대 클럭 속도는 거의 1/2로 감소한다. 또한 전력 소모는 크게 증가하는데, 이는 DRP 논리회로를 사용하고, mask 신호선이 스위칭 동작을 하기 때문이다.

## ■ Adiabatic logic을 이용한 DPA 대응방법

### ■ Adiabatic logic 개요 및 Efficient charge recovery logic(ECRL)

앞서 살펴본 SABL, WDDL, MDPL의 구조에서는 일반 CMOS 논리회로와 비교해서 두 배 이상의 전력이 소모되는 단점을 가지고 있다. 이러한 전력 문제를 해결하기 위해서 사용할 수 있는 방법이 adiabatic 논리 회로를 이용하는 것이다.

Adiabatic 논리회로란 기존 CMOS logic 동작의 전력을 감소시키기 위한 기술 중 하나로, 기존의 회로에서 접지로 방전되는 전하를 전원부로 회수하여 재사용하는 방법을 말한다. 여러 형태의 adiabatic logic 회로들이 발표되었으며, 그 중에서 efficient charge recovery logic(ECRL)은, 전력 제공을 클럭과 같이 사용한 supply clock을 사용하여 보다 효과적인 방법으로 전력을 감소시킨다.[6] 그 동작원리는 다음과 같다.

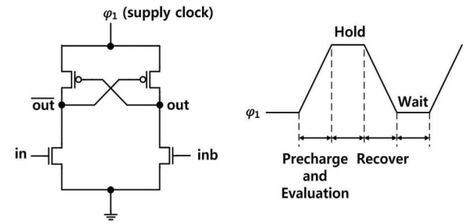



그림 8. Efficient Charge Recovery Logic inverter 및 supply clock

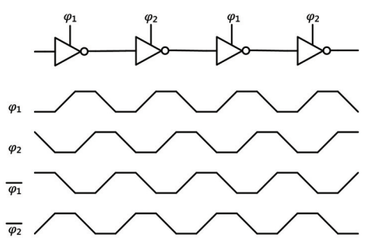



그림 9. Inverte chain과 4-phase supply clock

그림 8로부터 in, inb의 입력이 각각 '1', '0'을 갖는다면, supply clock이 precharge and evaluation 구간에서 φ1이 VDD로 상승하게 되면서 out, outb는 '0', '1'값을 갖는다. Hold 구간에서는 out, outb의 값이 다음 단의 입력으로 사용되기 위해 유지하고 있고, φ1이 하강하는 recover 구간에서는 outb로 충전된 전하가 접지로 방전되는 것이 아닌, φ1 노드로 하게 된다. 이와 같은 동작을 바탕으로 그림 9와 같은 4-phase supply clock을 사용하면, 이전 단의 값이 유지되고 있는 hold 구간동안 다음 단의 evaluation이 이루어지고, 동일한 과정에 계속 반복된다.

### ■ Symmetric Adiabatic Logic (SyAL)

DRP 논리회로를 이용한 방법이 전력소모가 많다는 단점을 보완하기 위해서 adiabatic logic을 살펴보았다. 그러나, ECRL방식의 Adiabatic logic 셀의 경우는 evaluation 구간에서 입력 데이터에 따라 전류가 방전되는 경로가 다르기 때문에 소비전력 패턴의 모습이 입력 데이터에 따라 다른 모습을 관찰할 수 있는 단점을 가지고 있다.

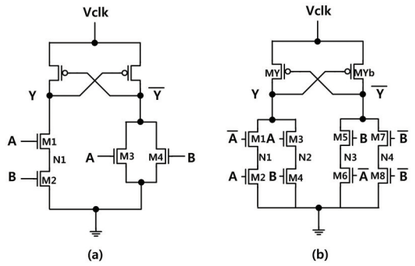



그림 10. Adiabatic Logic의 AND/NAND 게이트 회로도
(a) efficient charge recovery logic,
(b) symmetric adiabatic logic (SyAL), ver.1

| A | B | M1–M2 | M3–M4 | M5–M6 | M7–M8 |
|---|---|---|---|---|---|
| 0 | 0 | on–off | off–off | off–on | on–on |
| 0 | 1 | on–off | off–on | on–on | off–off |
| 1 | 0 | off–on | on–off | off–off | on–on |
| 1 | 1 | off–on | on–on | on–off | off–of |

표 1. 입력 데이터에 따른 SyAL 방전회로의 동작 상태

그림 10.(a)에서 Prechage 구간 동안 입력 A, B가 모두 '1'을 갖는다면 MYb 가 켜지고, Yb 노드가 충전되는 것을 알 수 있다. 하지만 A, B가 각각 '1', '0'의 입력을 갖는다면, MY 트랜지스터 뿐만 아니라 M1도 함께 도통되어, Y 노드 뿐만 아니라, N1 노드도 함께 충전되므로, A, B모두 '1'의 입력일 때와 다르게 N1 노드의 커패시턴스를 충전할 만큼의 전류를 추가로 소모한다는 것을 알 수 있다.

이와 같은 Y, Yb 노드의 방전 경로가 상이하여 입력에 따라 달라지는 소비전력을 동일하게 하기 위해 본 연구실에서는, 그림 10.(b)와 같이 대칭구조의 방전 경로를 갖는 adiabatic logic 회로를 제안하였다.[7] 표 1으로부터 A, B 입력에 따른 방전 경로 트랜지스터의 on-off 상태를 알 수 있으며, 4가지 경우 모두 동일한 상태를 갖는 것을 확인 할 수 있다.

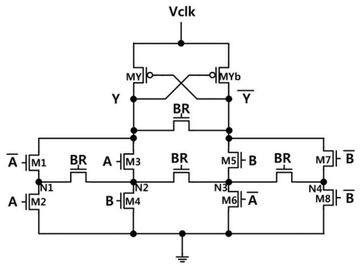



그림 11. Symmetric adiabatic logic의 AND/NAND 게이트 회로도, ver.2

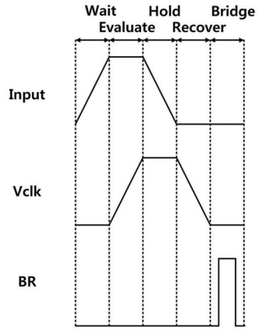



그림 12. Symmetric Adiabatic Logic의 타이밍 다이어그램

기존 adiabatic logic(ver.1) 에서 이전 입력 데이터와 무관하게 precharge하는 양을 동일하게 하기 위해서는 Y, Yb 뿐만 아니라 N1, N2, N3, N4 노드의 전하 공유를 통해 매 주기마다 동일한 조건의 adiabatic logic을 충전하는 것이 필요하다. 이를 위해 BR 신호를 통해 recover 구간 이후 Y, Yb 노드의 전하공유가 이루어지고, N1, N2, N3, N4 또한 동일한 동작을 수행하여 매 evaluate 동작 이전에 동일한 조건을 만들어준다. 그림 11에 BR 신호를 포함한 symmetric adiabatic logic의 AND/NAND 게이트 회로도를 나타내었고, 타이밍 다이어그램을 그림 12에 나타내었다.

■ 시뮬레이션을 통한 결과 분석

제안하는 symmetric adiabatic logic의 동작을 HSPICE 시뮬레이션을 통해 확인하였다. 입력 신호에 따른 전류 패턴을 기존 ECRL과 비교하여 그림 13에 나타내었다.

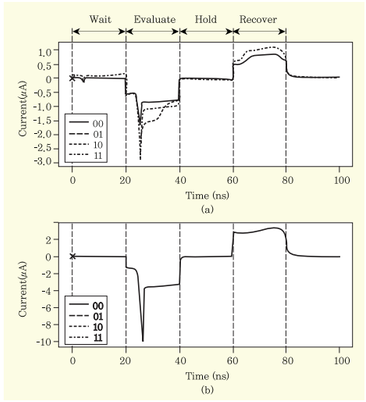



그림 13. ECRL과 SyAL에서의 입력 데이터별 소모전류 비교: (a) ECRL 에서의 소비 전류 (b) SyAL에서의 소비전류

그림 13 (a)를 통해서 입력 데이터에 따라서 소비되는 전류 패턴이 다르다는 것을 확인할 수 있는 반면 그림 13(b)에서는 모두 입력 데이터와 무관하게 모두 동일한 전류 패턴이 나타나는 것을 확인할 수 있다. 이러한 adiabatic logic 구조는 소비전력을 효과적으로 감소시키는 것과 동시에 입력 값과 무관하게 동일한 전력소모를 보여주므로, 보안용 소자의 DPA 대응에 효과적으로 적용할 수 있을 것이라고 예상한다.

## 결론

보안용 소자의 다양한 공격 방법 중에서도 DPA는 보안 정보 값의 소비 전력을 통계적인 방법을 이용하여 분석하는 저비용의 강력한 공격 수단이다. DPA 공격에 대해 셀 레벨에서 이루어지는 기존의 대응책으로 DRP를 이용한 SABL, WDDL, MDPL 등이 개발되었으나, 전력 소비가 크다는 단점을 가지고 있다.

이러한 문제를 해결하기 위하여, adiabatic logic에 기반한, 새로운 DPA대응 회로 설계 기법인 Symmetric Adiabatic Logic (SyAL)을 제안하였다. 이 논리회로에서는 입력 데이터와 소비전력과의 상관관계를 없애기 위하여 방전 경로를 대칭적인 구조로 만드는 것 뿐만 아니라, 내부 노드의 전하 공유를 통해서 매 클럭이 시작하기 이전에 출력 및 내부 노드를 모두 동일한 조건으로 만들어주어, 충/방전 구간에 동일한 전류가 소모된다. 이러한 SyAL 방식의 구조는 DPA 공격에 대한 방어에 매우 효과적으로 사용할 수 있을 것으로 기대된다.

## Reference

[1] P.Kocher, J.Jaffe, and B.Jun, "Differential Power Analysis", Proc. Advances in Cryptography, 1999, pp. 388–397
[2] K.Tiri and I.Verbauwhede, "Place and Route for Secure Standard Cell Design", 2004, Sixth International Conference on Smart Card Research and Advanced Applications, pp.143–158
[3] K.Tiri, M.Akmal, and I.Verbauwhede, "A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards, 2002, European Solid-State Circuits Conference, pp.403–406
[4] K.Tiri, and I.Verbauwhede, "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation", 2004, Design, Automation and Test in Europe Conference and Exposition, vol. 1, pp.246–251
[5] T.Popp, and S.Mangard, "Masked Dual-Rail Pre-Charge Logic: DPA-Resistance without Routing Constraints", 2005, Cryptographic Hardware and Embedded Systems, vol. 3659 of Lecture Notes in Computer Science, pp. 172–186
[6] Y.Moon, and D.K.Jeong, "An Efficient Charge Recovery Logic Circuit", Journal of Solid-State Circuits, vol. 31, no.4, 1996, pp.514–522
[7] B.D.Choi, K.E.Kim, and D.K.Kim, "Symmetric Adiabatic Logic Circuits against Differential Power Analysis", ETRI Journal, vol. 32, no. 1, pp. 166–168

# 차량 인식 기술 소개

한양대 지능형 차량용 SoC 플랫폼 센터
(http://idec.hanyang.ac.kr)
주 소 : 경기도 안산시 상록구 사3동
한양대학교 에리카캠퍼스 3공학관 321호
CEO : 신현철 교수
shin@hanyang.ac.kr
행정팀 : 윤진은 행정원
jeyun@idec.hanyang.ac.kr
031-400-4079

## 서론

무인 운전 또는 자동 운전은 더는 꿈이나 공상과학 얘기가 아니다. 지난 2012년 5월에 미국 네바다 주에서 구글 무인 운전 자동차가 테스트에 통과하여, 무인 운전 자동차 운전 면허증을 발급받았다. 여러 도로 상황에서 1만 마일 이상 무인 주행한 기록이 있으면 면허 심사를 신청할 수 있으며, 무인 운전 대중화를 위한 경쟁이 시작되었다.

스마트 차량의 실용화를 위한 여러 영상 비전 관련 연구가 진행 중이다. 도로 위의 다른 차량, 보행자, 건물 등을 인식하기 위해서, 수동적인 센서인 카메라에서부터 능동적인 센서인 레이저까지 다양한 각도에서 접근하고 있다. 그러나 능동적 센서가 다른 기기에 비해 상대적으로 고가이며 가까운 거리를 측정할 수 없는 등의 단점들을 가지고 있어서, 여기에서는 수동적 센서인 차량용 카메라를 이용한 영상 비전으로 개발된 다양한 차량 인식 기술을 소개하기로 한다.

## 본론

최근 위험 상황에서 운전자에게 경고를 주기 위한 Advanced Driver Assistance Systems (ADAS) 가 부각 되고 있다. 하지만 ADAS 시스템은 실시간으로 이미지 데이터를 처리하므로 많은 연산량을 처리할 수 있는 시스템이 요구된다. ADAS 시스템의 차량 인식에서는 두 가지 단계의 전략을 사용하여 연산량을 줄인다. 첫 번째 단계에서 잠재적인 차량을 초기 후보자로 선정하여 차량이 아닌 부분에 대한 불필요한 연산들을 막을 수 있다. 두 번째 단계에서 그 후보들을 참인 값과 거짓인 값으로 분류하는 방법을 사용한다. 이를 통해 많은 연산량을 줄일 수 있다.

인공적인 물체들의 중요한 특징 중 하나인 대칭도 차량 인식에서 광범위하게 활용되고 있다. 많은 연구에서 차량의 정면 및 후면이 대칭이라는 점을 차량 인식에 사용하고 있다. 하지만 이 접근 방법은 대칭을 특징으로 사용하지 못하는 일부 차량 영상들에서 문제가 생길 수 있다. 이 문제를 보완하기 위해 에지 정보와 색상 정보로 차량을 인식하고 배경을 세분화하여 차량 인식하는 방법이 제시되었다. 또한, 그림자를 이용한 차량 인식 방법도 연구되었다.

그림 1에서 보이듯 차량의 아랫부분은 그림자로 인해 주변의 다른 영역보다 어둡게 보인다. 그림자를 차량을 인식하는데 사용할 수 있으나 이 접근 방법에는 그림자를 구분할 수 있는 특정 임계값을 설정해야 한다는 문제점이 있다. 이 외에도 일반적인 에지 검출 방법으로 수평 에지, 수직 에지 혹은 모두를 사용하여 차량의 왼쪽과 오른쪽의 위치를 찾는 방법도 있다. Sobel 에지 필터 또는 라플라시안, 가우시안, 캐니 에지 검출 방법 등이 사용된다. 영상 처리 시간을 줄이기 위해 Look Up Table, 멀티 스케일 검색 방법을 도입하기도 한다.

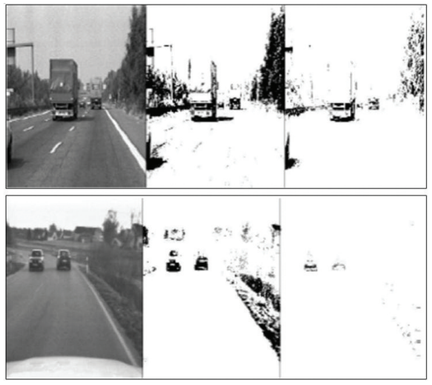


그림1 . 다양한 형태의 차량과 그림자 형상

에지와 색상 정보를 이용하여 차량을 인식하는 방법과 달리 일부 연구에서는 상위 수준의 방법으로 차량 인식 문제에 접근하였다. 자동차량인식을 위한 Principal Component Analysis (PCA), Independent Component Analysis (ICA) 를 함께 사용하기도 하며, 트레이닝 시간을 줄이기 위해 AdaBoost 알고리즘을 개선한 방법도 사용한다. Latent Support Vector Machine (LSVM) 과 Histogram of Oriented Gradients (HOG) 을 사용한 차량 인식 방법도 제안되었다.

트레이닝 과정과 픽셀값 차이를 이용하여 특징점을 찾는 이 방법은 98%의 높은 차량 인식률을 보인다. Gabor 필터로 서로 다른 방향에서의 차량의 특징이 되는 에지를 추출하여 차량을 인식하는 방법도 제안되었다. Gabor 필터와 Support Vector Machines (SVM) 를 혼합하여 사용한 방법은 90% 이상의 인식 결과를 보였다.

최근에는 능동적인 학습 프레임워크 방법이 차량 인식 과정에서 사용되었다. 테스트 과정에서 얻은 영상을 트레이닝 영상으로 추가해서 사용하는 능동(active) 방법은 높은 정밀도와 인식률을 가진다. 그림 2는 학습과 SVM 분류기를 사용한 차량 인식 방법을 보여준다.

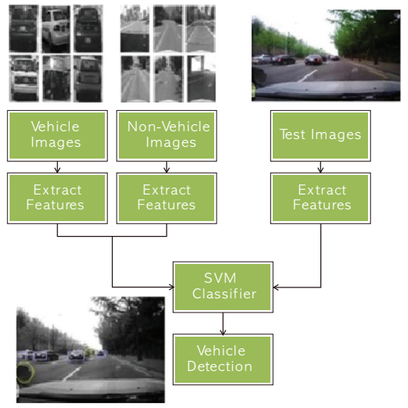



그림2 . SVM을 이용한 차량 인식

우리 연구실에서는 상위 수준의 특징 (Bag-of-feature) 과 하위 수준의 경계선을 결합한 차량용 블랙박스 카메라 기반의 새로운 차량 인식 시스템을 개발하였다. 여기에서는 정확한 에지 정보를 얻을 수 있는 새로운 에지 검출 방식인 Bigaussian Edge Detection (BED) 을 제안하였다.

Canny 에지 검출기는 에지 필터에 비교적 최적화된 방법으로 알려졌다. 하지만 Canny 방법은 low-pass 필터링을 할 때 사용한 임계값에 따라서 에지가 변형되거나 노이즈가 많이 남아 있는 단점이 있다. 제안한 에지 검출 방법은 비선형적인 Bilateral 필터를 이용한 영상 범위 내에서 정확한 위치에 에지를 강조하고 노이즈를 제거하는 성질을 가지고 있다. 제안한 방법을 차량인식에 적용하였을 때 Canny 에지 필터보다 현저하게 좋은 결과를 얻었다.

BED 기반의 에지 검출의 기본 아이디어는 영상에서 픽셀 사이의 기하학적 거리와 휘도 차를 동시에 고려하는 필터링 방법으로 영상에서 노이즈를 제거하는 동시에 위치가 정확한 에지를 찾는 것이다. 노이즈를 제거하기 위하여 아래 수식 (1)과 같이 공간 도메인에서 기하학적 거리에 따른 weight를 이용한다.

$$g(p-q) = e^{-\frac{1}{2}\left(\frac{\|p-q\|}{\delta_d}\right)^2} \quad (1)$$

이와 동시에 에지를 검출하기 위하여 수식 (2)와 같이 인자 사이의 휘도차에 관한 함수를 휘도 범위에서 적용한다.

$$h(I_p - I_q) = 1 - e^{-\frac{1}{2}\left(\frac{\|I_p - I_q\|}{\delta_r}\right)^2} + \alpha \quad (2)$$

위의 두 수식을 조합하면 수식 (3)을 얻을 수 있다.

$$J_p = \frac{1}{K_p}\sum_{q\in\Omega} I_q\, g(p-q)\, h(I_p - I_q) \quad (3)$$

수식 (3)에서 p는 기준 픽셀이고 q는 그 이웃 픽셀 중 하나이며 Ip와 Iq는 각각의 휘도 값을 나타낸다. $\alpha$는 Ip를 Iq로 나눈 값이 0이 되는 것을 방지하기 위한 오프셋이다.

경계부분에 있는 밝은 면의 픽셀을 중심으로 필터링하면 어두운 부분에는 높은 가중치를 주게 되고 밝은 부분에는 0에 가까운 가중치를 주게 된다. 반대로 어두운 픽셀을 중심으로 필터링했을 때에는 밝은 부분에 더 높은 가중치가 부여된다. 그러므로 이 필터는 공간 도메인에서는 low-pass filter로서 노이즈에 의한 픽셀 사이의 작은 차이를 평균화시키며, 동시에 휘도 도메인에서는 주변 픽셀의 휘도차이가 강조되는 표준 high-pass filter의 역할을 한다. 그림 3은 BED 기반의 차량 검출 방법과 Canny 기반의 차량 검출 방법의 인식 결과를 비교한 그림이다. BED가 우수함을 알 수 있다. 이 기술은 영상처리에 폭넓게 활용할 수 있으며, 특허출원하였다.

에지 정보를 사용하여 초기 후보영역을 얻고 Bag-of-Features (BoF) 알고리즘으로 차량의 특징을 묘사하였으며 K Nearest Neighbor (KNN) 방법으로 트레이닝된 데이터와 테스트 데이터를 비교하여 차량을 인식한다.

그림 4의 BoF 는 텍스트 검색을 위한 모델링에서 파생되었다. 이를 테면 의학서적에는 질병, 약과 같은 단어들이 빈번히 나타나고, 농업서적에는 농작물 등 단어들이 빈번히 나타난다. 이런 원리를 영상에 적용하여 영상 속의 어떤 특징이 많이 나오는지를 판단하여 물체를 인식하는 방법이다. BoF 알고리즘은 특징 생성, 분류 및 테스트 3개 과정으로 나눌 수 있다. BoF 모델링은 트레이닝 이미지 히스토그램을 생성하고 테스트 이미지들의 히스토그램과 비교하여 수행된다. 이 방법의 주된 장점은 계산의 단순성과 효율성, 그리고 affine 변환에 불변성을 갖고 있다는 것이다.

KNN 알고리즘은 패턴 분류에 이용되는 직접적인 통계 방법이다. 우선 H를 학습데이터라고 하면 H는 일정한 차원의 벡터들로 구성되어

있다. 만일 동일한 차원인 미지의 벡터를 분류할 경우, 그 벡터와 가장 가까운 거리에 있는 K개의 벡터들을 선택한다. 여기서 벡터 간의 거리는 Euclidean norm을 사용한다. 주어진 영상과 차량 영상의 히스토그램 비교를 통하여 비교적 일치하는 경우에는 차량으로, 아닌 경우에는 차량이 아닌 것으로 판단하는 부분에 KNN 알고리즘을 사용한다.

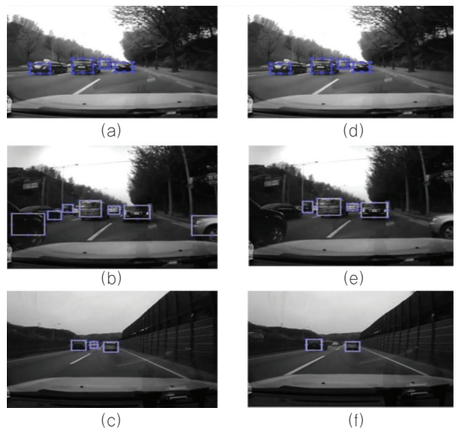



그림 3. BED를 사용한 차량 인식 방법과 Canny 방법 비교
(a)~(c) Combining BED and BoF,
(d)~(f) Combining Canny and BoF

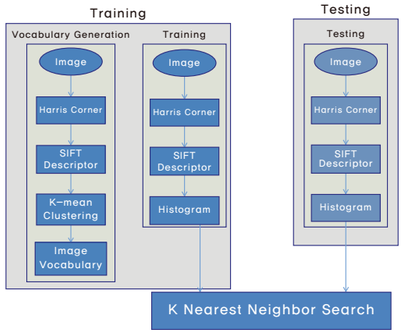



그림 4. BoF 및 KNN 알고리즘을 이용한 차량 인식

앞서 주로 주간을 기준으로 차량 인식에 대해 설명하였다. 그러나 주간에만 차량을 운전하는 것이 아니며, 최근 통계에서 야간에서의 차량 주행 환경이 도로 교통안전을 위협하는 큰 원인으로 알려졌다. 유럽에서는 거의 약 32.7%의 교통사고가 야간에 발생한다고 밝혀졌다. 소비자들이 교통안전의 중요성을 의식하면서 첨단 운전자 보조 시스템 ADAS 에 대한 시장수요와 소비자들이 대폭 늘어나고 있다. 그리고 많은 자동차 회사들이 Automatic Cruise Control 시스템을 개발했으며 현재도 개발 중이다. 이러한 기술에서 야간 전방차량 인식의 주된 특징으로 후미등과 제동 표시등을 이용한다(그림5 참조). 하지만 차량 모델에 따라 후미등과 제동 표시등의 모양이 천차만별이므로 인식하기에 많은 어려움이 있다. 최근에 많은 연구가 진척되어 차량을 인식하고 추적하는 방법을 통해 비교적 높은 인식률을 보이고 있다.

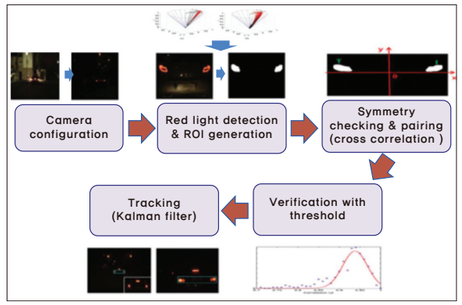



그림 5. 후미등을 이용한 야간 차량인식 방법

일반적인 방법은 아래와 같다.

◆ 카메라 노출강도를 국제표준 EVISO 10으로 조절하여 후미등의 밝은 부분이 포화 되지않게 한다.

◆ 다음 HSV 색도 공간에서 빨간색에 관한 규정을 정하여 야간 도로에서의 다른 색상의 밝은 물체와 구분한다.

◆ 빨간색을 검출하면 그 부분을 관심영역으로 설정하고 서로 대칭되는 후미등의 특징을 이용하기 위해 cross correlation 을 계산하여 symmetry checking을 한다.

◆ Pairing 된 후미등을 추적하는 방법으로 인식률을 제고한다. 이 방법을 이용하여 각각 세 개의 이미지 시퀀스에 대하여 실험한 결과 평균 97.2%의 차량인식률을 보였다.

## 결론

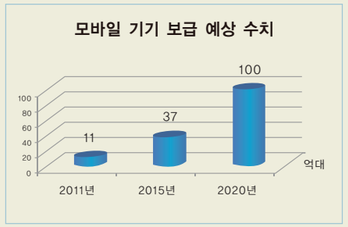
저조도 환경인 야간에서는 visible sensor의 활용이 제한된다. 이 점을 보완하기 위하여 최근에는 장애물과의 거리를 측정할 수 있는 RADAR 나 LIDAR를 결합하는 방법을 사용하거나 근적외선 카메라를 이용하여 열 영상으로부터 물체를 인식하는 방법도 사용한다. 그러나 열 영상 카메라는 해상도가 낮으며 색상 정보를 가지고 있지 않는 단점이 존재한다. 이러한 단점을 서로 보완하기 위하여 visible 영상과 열 영상을 결합한 퓨전센서 기반 야간 인식 방법도 활발히 연구, 개발되고 있다.

SPECIAL Column I

# 「모바일 기기의 융합시대: 모바일-AP IDEC 플랫폼 센터 (IPC)」

*모바일 기기가 모바일 인터넷 대중화 시대를 열고 있다. "스마트폰으로 하루를 시작하여 스마트폰으로 마감한다."는 소비층이 등장할 정도로 스마트폰 및 모바일 기기의 영향력이 커지고 있다. 2011년 스마트폰 보급 대수는 약 7.3억대, 스마트폰을 제외한 모바일 기기는 약 3.6억대로 Gartner 조사를 바탕으로 예측한 2015년 전체 모바일 기기는 37억대, 2020년에는 100억대로 늘어날 전망이다. 모바일 기기는 실시간(Real-time), 정보 · 소통의 무한 확장(Reach), 공간 제약을 극복한 실제감(Reality) 등 '3R'을 통해 개인 · 기업 · 사회를 변화시킬 것이다.*

모바일 기기가 모바일 인터넷 대중화 시대를 열고 있다. "스마트폰으로 하루를 시작하여 스마트폰으로 마감한다."는 소비층이 등장할 정도로 스마트폰 및 모바일 기기의 영향력이 커지고 있다. 2011년 스마트폰 보급 대수는 약 7.3억대, 스마트폰을 제외한 모바일 기기는 약 3.6억대로 Gartner 조사를 바탕으로 예측한 2015년 전체 모바일 기기는 37억대, 2020년에는 100억대로 늘어날 전망이다. 모바일 기기는 실시간(Real-time), 정보 · 소통의 무한 확장(Reach), 공간 제약을 극복한 실제감(Reality) 등 '3R'을 통해 개인 · 기업 · 사회를 변화시킬 것이다.



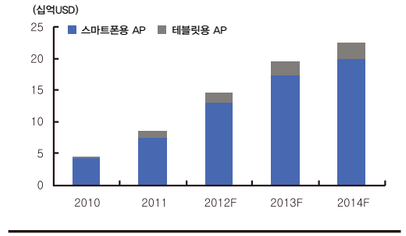

먼저 역사상 가장 강력한 정보력과 네트워크 파워를 가진 모바일 세대가 등장할 것이다. 기존의 정보 · 미디어 소비가 디지털 소비 형태로 급격히 전환되고, 모바일 오피스족의 확대로 기업경영은 물론 건축 · 도시 설계 · 교통흐름 등도 변화할 것이다. 또한, 모바일 커뮤니티를 통해 실시간 소통이 증가하면서 여론 형성 및 사회적 커뮤니케이션이 저변과 속도도 획기적으로 개선될 것이며, 新시장 · 新비즈니스 모델의 출현이 가속화될 것으로 기대된다.

전 세계 스마트폰 애플리케이션 시장은 2013년 295억 달러로 2010년(68억 달러)에 비해 4배 이상 성장할 것으로 보인다. 모바일 광고 · 아이템 판매 · 유료 서비스 등의 수익모델 하에 게임 · 소셜 네트워크서비스(SNS), 모바일 쇼핑 등이 성장할 것이며 모바일 기술이 전 산업 분야에 접목되면서 미디어, 자동차, 교육, 소매 등 전 산업의 혁신을 가져올 것으로 예상한다.

최근 모바일 플랫폼은 단순히 애플리케이션을 구동시키는 기능에서 벗어나 하드웨어와 결합한 콘텐츠 및 서비스, 마케팅, 유통, 의료, 개인화 정보 공유의 기능으로 발전하고 있다. 이는 모바일 기기의 부가가치를 증대시키고, 적용 분야를 다양화할 수 있기 때문에 새로운 산업을 발생시켜 경제 및 라이프 스타일 등 사회 전 분야에 걸쳐 매우 큰 파급 효과를 불러올 것이다.

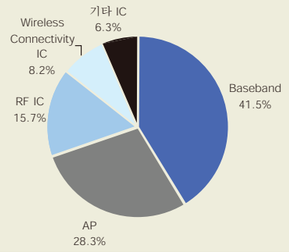
[삼성전자 S.LSI 분석 자료 : 스마트폰 및 태블릿용 AP의 가파른 성장세를 확인할 수 있다. 따라서 모바일-AP 플랫폼의 교육적, 사업적 가치는 향후 모바일 분야에 매우 큰 영향을 줄 수 있다.

### 스마트폰과 Tablet PC AP시장 규모




주 : Snap Dragon과 같은 One Chip도 포함한 수치
자료 : Gartner

### 전체 휴대폰 System LSI 수요 비중 (2011)

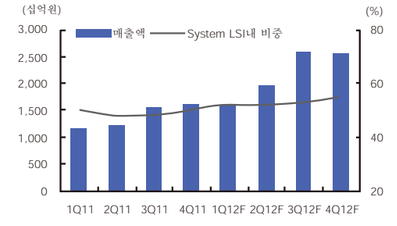



주 : 금액 기준
자료 : Gartner, HMC투자증권

### 삼성전자 스마트폰용 AP와 Baseband


자료 : 삼성전자, HMC투자증권

### 삼성전자 AP 매출액 추이

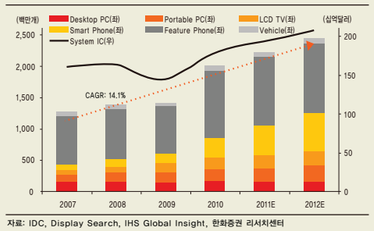



자료 : 삼성전자, HMC투자증권

또한, 스마트폰 및 모바일 기기의 빠른 확산으로 모바일 Soc의 수요가 급격히 증가하고 있으며, 국내 삼성전자 System LSI 매출은 2011년도에 전년도 대비 45% 증가하여 16조 가량을 기록하였다. 2012년 전 세계 Foundry 시장은 스마트폰 관련 System LSI 및 Apple 등의 Foundry 수요 증가에 힘입어 전년 대비 4% 이상 성장할 것으로 예상한다.

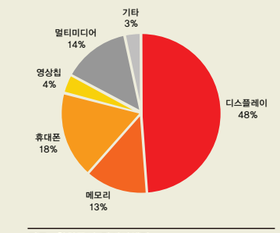
(동부 하이텍) 그리고 2011년 상반기 국내 팹리스 업종별 매출 총액에서 휴대폰은 18%의 비중을 차지하고 있으며(디스플레이의 비중이 50% 가까이 되는 이유는 LCD 패널 드라이버 IC의 공급 물량 때문), 시스템 반도체의 년 출하량 변화를 살펴보면 스마트폰과 태블릿 종목이 다른 분야에 비해 꾸준히 성장하고 있음을 알 수 있다.

**시스템반도체는 전방산업 출하량과 매우 높은 상관성**




자료: IDC, Display Search, IHS Global Insight, 한화증권 리서치센터

**2011년 상반기 국내 팹리스 상장사 업종별 매출총액**




자료: 한화증권 리서치센터

이에 경북대학교 모바일-AP 플랫폼 센터는 Mobile-AP를 통하여 다양한 핵심 IP를 개발하고 국내 다수의 팹리스 기업으로의 기술이전 및 인적교류를 실현하며 산학협력 네트워크를 이용하여 Mobile 플랫폼 산업을 선도할 통합적 인재 양성 활성화에 이바지할 것이다.

본 플랫폼 센터는 IT와 에너지, BT의 융합기술을 이용하여 시간과 공간에 구애받지 않고 언제 어디서나 전원 충전 걱정 없이 건강과 생활을 관리하는 확장형 Mobile-AP 플랫폼을 개발하고자 한다. 이에 Mobile-AP 기술영역 중 핵심 사업 (Mobile Application Processor, 모바일 소프트웨어, 무선 에너지 전송 WPT(Wireless Power Transfer), U-헬스케어(Bio/Health Technology))을 대상으로 추진 및 육성하여 모바일-AP 개발 및 응용 분야의 기술 플랫폼 개발과 발전에 이바지하고자 한다.

| 구 분 | 내 용 |
|---|---|
| 교재 및 교육과정 개발 | ■ 모바일-AP H/W platform<br>■ 모바일 interface 및 Bio-sensor<br>■ 무선 에너지 전송 및 충전 기술<br>■ U-헬스케어 구축을 위한 platform<br>■ 모바일-AP 임베디드 소프트웨어<br>■ 3년간 총 10권 교재 및 10개 교육 과정 개발 |
| 교육기자재 개발 | ■ 모바일-AP 용 platform 보드 개발<br>■ HFSS S/W를 활용한 공진기 Simulation 교보재 개발<br>■ U-헬스케어 구축을 위한 platform 개발<br>■ 접촉/비접촉 센서 및 카메라를 활용하는 모바일기기 제어 프로그램 개발 |
| 강좌개설 | ■ 모바일-AP platform 관련분야의 요소기술<br>■ 모바일 interface 및 Bio-sensor 관련분야의 요소기술<br>■ 무선 에너지 충전 Station 설계 기술<br>■ U-헬스케어 구축을 위한 관련분야의 기초 및 요소기술<br>■ 모바일-AP 임베디드 S/W 관련분야의 기초 및 요소기술<br>■ 3년간 총 30강좌 개설 및 총 10 회 세미나 개최 |

본 센터는 교수, 기업체 연구원, 학생, 대학 인력으로 구성된 교육과정 개발위원회를 중심으로 교육과정을 개발해 나갈 예정이다. 지금까지는 간단한 설문조사 결과나 일부 기업의 의견이 교육과정에 반영되었으나 앞으로는 대기업, 중소기업, 교수, 최근 졸업생의 의견을 충분히 반영해 교과 과정을 개발하고, 개발된 Mobile-AP platform을 적극 활용하는 교육과정을 만들어 나갈 것이다. 또한, 기업과 학생의 의견을 지속적으로 monitoring 하여 교육과정에 반영할 것이다.

교재 개발은 이론에 관한 책은 세계적으로 유명한 학자들이 이미 집필하였으므로 이론적인 내용을 편집하는 융합형 교재 개발은 지양하고 실험실습을 통하여 이론을 확인 · 다양한 이론을 융합할 수 있는 능력을 키우는 교재 개발을 지향해 나갈 것이다.

| 구 분 | 내 용 |
|---|---|
| Core-A 기반 모바일-AP H/W platform 개발 | ■ Core-A 기반 H/W platform 설계<br>■ H/W Platform 구축을 위한 IP 개발 및 모바일-AP 설계<br>■ OS Porting(u-OS, Linux, Android)<br>■ 검증용 SOC 및 S/W 개발 |
| 모바일 interface 개발 및 Bio-sensor 연구 | ■ 모바일 Interface(Bluetooth, RFID, NFC) 환경 개발<br>■ Bio-Sensor 적용 및 설계(ECG센서, 혈당센서)<br>■ H/W Platform을 위한 PMIC(SIMO) 개발 |
| 무선 에너지 충전 Station 개발 | ■ 무선 에너지 충전 Station 개발<br>■ 안정적 전원 관리를 위한 IP 개발<br>■ 전송 효율 상승을 위한 능동 임피던스 매칭 H/W 개발 |
| U-헬스케어 platform 개발 | ■ 뇌파와 심전도를 측정하기 위한 저전력/저면적과 고사양 Instrumentation Amplifier IP 구현<br>■ 뇌치필터 IP 구현 |
| 모바일-AP 임베디드 소프트웨어 개발 | ■ 안드로이드 플랫폼 기반 멀티미디어 임베디드 소프트웨어 개발<br>■ 모바일 GPU를 활용하는 임베디드 소프트웨어 개발<br>■ Core-A 플랫폼 기반 임베디드 소프트웨어 개발 |

〈교육개발 및 운영〉

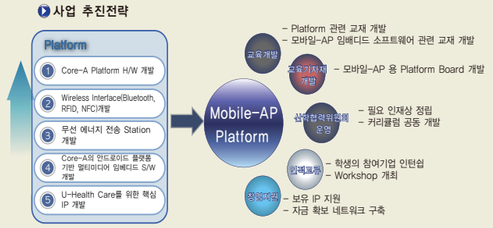
연구 개발은 제한된 리소스로 mobile platform 전체를 연구하는 것은 어려우므로 안드로이드 OS에서 임베디드 SW 개발, 추출 또는 가공된 정보를 모바일 기기로 전송할 수 있는 platform을 구축하고, 연구진을 Core-A 기반 platform 개발, 무선 에너지 스테이션, 모바일 인터페이스, U-헬스케어, 임베디드 S/W 그룹으로 구성하여 platform 구축에 필요한 기술을 개발하고 연구된 모든 기술은 H/W와 S/W 형태로 IP화하여 platform에 이식하여 활용할 계획이다.

| 구 분 | 내 용 |
|---|---|
| 산학협력위원회 운영 | ■ 필요 인재상 정립<br>■ 공동 연구 분야 발굴 및 개발 IP의 산업화<br>■ 커리큘럼 공동개발 |
| 인적교류 | ■ 학생의 참여기업 인턴쉽<br>■ 학생인력 및 기업인력 재교육을 위한 상호 강사지원<br>■ Workshop 연 1회 개최<br>■ 화상회의 수시 개최<br>■ 전체 회의 연 4회 개최<br>■ 사업 성과 발표회 연 1회 개최 |
| 창업지원 | ■ 보유 IP 지원<br>■ 자금 확보 네트워크 구축 |

〈교육개발 및 운영〉

산학 연계에는 참여 기업, 참여 교수를 중심으로 산학협력위원회, 교육과정 위원회를 구성하여 공동 연구 분야 발굴, SOC 인재양성 방향정립, 교과 과정 등을 협의할 예정이다. 또한, 참여기업이 대부분 경인지역에 있으므로 서울에서 정기적인 교류회를 개최하고 1교수 1기업 멘토 시스템을 도입하여 실질적인 협력 시스템을 구축해 나갈 것이다.

**사업 추진전략**




〈산학 연계 네트워크〉

경북대학교 모바일-AP 플랫폼 센터는 총 12개 대학과 10개 기업의 63명이 모바일-AP IPC 사업에 참여한다. 스마트폰 및 모바일 기기의 빠른 확산으로 인해 모바일 SOC의 수요가 급격히 증가하고 있으며 모바일 관련 신기술에 대한 부가가치 또한 증가하고 있다. 그러므로 현재 모바일 기기가 가지는 공간 및 기술적 제약으로 인해 사용자가 필요로 하는 모든 기능을 구현하기 불가능한 상황을 모바일-AP의 설계와 확장성을 통해 해결하는 것이 시급한 과제라 할 수 있다.

경북대학교 모바일-AP 플랫폼 센터는 위에서 언급한 '교육개발 및 운영', '연구 개발', '산학 연계'를 통해 앞으로 확장형 Mobile-AP 플랫폼을 개발하고 향 후 대한민국의 Mobile 플랫폼 산업을 선도할 통합적 인재를 양성해 나가고자 한다.

경북대 모바일-AP 플랫폼 센터
(http://idec.knu.ac.kr/)
주 소 : 대구광역시 북구 산격동 1370번지
경북대학교 IT대학 3호관 406호
CEO : 최준림 교수 (jrchoi@ee.knu.ac.kr)
행정팀 : 변보련 행정원
ipc-mobile@ee.knu.ac.kr / 053-950-6858


*IEEE CASS(Circuits and Systems Society)는 매년 (ISCAS: International Symposium on Circus And Systems) 국제학술대회를 주관한다. 1968년 미국 마이애미를 시작으로 매년 개최되는 ISCAS 국제학술회의는 1963년 설립된 국제전기전자 학회인 IEEE (Institute of Electrical and Electronics Engineers) 주관 국제학술대회 중 가장 역사가 긴 학술대회이다.*

# IEEE ISCAS 2012 최초 한국 개최를 무사히 마치고

IEEE CASS(Circuits and Systems Society)는 매년 (ISCAS: International Symposium on Circus And Systems) 국제학술대회를 주관한다. 1968년 미국 마이애미를 시작으로 매년 개최되는 ISCAS 국제학술회의는 1963년 설립된 국제전기전자 학회인 IEEE(Institute of Electrical and Electronics Engineers) 주관 국제학술대회 중 가장 역사가 긴 학술대회이다. 또한, IEEE CASS에서 주관하는 IT, 반도체 및 응용분야의 국제학술회의로 세계 최대 규모이다. 현재까지 미국 26회, 캐나다와 일본 각 3회, 영국과 프랑스 각 2회, 독일, 스위스, 호주, 대만 등이 각 1회씩 개최하였으며, 한국에서는 이번에 처음으로 개최되었다. 명실상부 IT 선도국인 우리나라의 위상을 생각하면 섭섭한 대목이 아닐 수 없다.

IEEE는 현재 160개국에 40만 명의 회원과 1,800개의 지부를 운영하고 있다. 필자가 회장을 역임하고 있는 IEEE CASS 한국 지부는 국내의 산학연 전문가 집단으로 구성되었으며, ISCAS 2012 국제 대회 유치로 회원 증대 및 인지도가 급증, 권위 있는 학술 조직으로 성장하고 있다. 우리나라는 세계 첨단의 전자산업을 보유한 IT 강국임에도 불구하고 국내 산학연 단체의 국제전기전자 학회에서의 활동은 상대적으로 미흡하였다. 이러한 상황을 개선하고 더욱 적극적인 국제학회 활동을 이끌어 내어 국내 관련 기술 발전을 도모하기 위해, 세계 최고학회인 ISCAS 2012 한국 유치는 필수적이었다. 필자는 대내외적 요청을 받아 IEEE CASS 한국지부를 중심으로 유치위원회를 구성 여러 교수와 함께 제안서를 준비했고 정부와 기업들이 지원하였다. 마침내 2008년 시애틀 선정 회의에 첫 도전장을 내밀어 한국, 중국, 핀란드, 캐나다, 호주 등 5개국의 치열한 경합 끝에 다년간 유치 신청을 했던 다른 나라들을 제치고, ISCAS 2012 개최지로 만장일치로 선정되는 쾌거를 거두었다. 우리나라의 반도체 회로 및 시스템 기술을 세계 최고 전문가 집단에 알리고, 기술 경쟁력을 강화할 절호의 발판을 마련하였다.



ISCAS 2012는 5월 20일부터 23일까지 서울 COEX에서 거행되었는데, 전후 일정을 포함한 총 행사 일정은 6일이었다. 5월 18일부터 시작된 IEEE CASS BoG(Board of Governors) 미팅, ExCom(Executive Committee) 미팅을 포함하여 본격적인 ISCAS 행사인 일요일 전야제, 세계적 석학들의 초청 특강 및 900여 편의 논문발표, 그리고 행사 전후에 관광 프로그램을 지원하여 세계 기술 및 문화 교류에 지대한 영향을 미친 것으로 기대한다.

우리나라의 메모리 반도체 분야는 세계 최고수준의 기술과 시장을 선도하고 있으나, 가장 핵심 부품인 시스템 반도체 분야는 선진국보다 뒤져 있고 대만에도 뒤져있는 실정이다. 따라서 ISCAS 2012에서는 세계적 수준의 기술과 인적 교류를 통해 국내 반도체 및 시스템 기술 발전을 기대할 수 있을 뿐만 아니라 한국의 반도체 회로 및 시스템 기술과 IT 선도국의 위상을 세계 최고의 전문가 집단 (Opinion Leader)에게 알릴 수 있는 좋은 기회였다. ISCAS 2012 개최는 시스템 반도체의 기술을 한 단계 높이기 위한 최고의 기회로 인식되어 지식경제부, 서울시, 한국관광공사, 삼성전자 등 여러 기관에서 전폭적으로 후원하였다.

ISCAS 2012의 학술 주제는 Convergence of BINET (Bio, Info, Nano, Enviro Technology)으로 바이오, 정보, 나노, 환경 기술의 융합이며, 시스템 반도체 기반의 정보통신기기, 자동차, 바이오 관련 제품 등 우리나라의 주력산업을 고도화하고, 미래 신성장동력 산업 발굴에 크게 이바지할 것이다. 이에 맞춰 한국 시스템 반도체의 선구자인 삼성전자 우남성사장, 3D 트랜지스터의 발명가인 UC Berkeley의 Cheming Hu 교수, Bio분야의 석학인 TU Berlin의 Roland Thewes 교수의 기조연설이 진행되었다. 또한, 17개의 정규 분야 및 최신 기술을 다루는 특별세션이 마련되어 세계 각국으로부터 제출된 1,800여 편의 논문으로부터 엄선된 우수 논문에 한하여 구두 발표 및 포스터 발표를 하여 국제적 기술교류의 장으로 열었다. 더불어 관련 전문가를 초빙하여 해당 분야의 최신 지식을 배울 수 있는 튜토리얼도 제공되었다. 따라서 관련 기업, 연구소 및 학교의 구성원이 이번 학회 참석을 통해 최신 관련 기술 습득 및 향상에 큰 도움이 되었다고 믿는다.

특히 삼성전자 우남성 사장의 첫째 날 기조연설인 "Smart Mobile Devices and Semiconductor Solution: Past, Present and Future" 발표 내용이 훌륭하여 학회 행사 내내 회자되었고, 각 세션의 구성이나 진행, 우수한 논문의 질 등으로 말미암아 이전 ISCAS와 달리 마지막 날까지 논문 발표장마다 빈자리가 없을 정도로 참가자들의 열기가 고조되어 많은 연구자에게 훌륭한 기술교류의 장을 제공하였다. 또한, 이전의 외국에서 개최된 ISCAS와 달리 삼성전자의 전시 부스에 대규모 최첨단 제품들을 전시해서 많은 외국 참가자가 한국의 IT 기술력에 감탄하였으며, 전체적인 전시부스에 많은 관람객을 흡인하는 효과를 가져왔다. 또한, Live Demo 세션도 과거와 달리 많은 참가자들이 관람하여 성황을 이루었다.

이번 ISACS 2012에는 전 세계에서 1,200여 명이 참가하여 학술발표뿐만 아니라 전시, 초청강연, 한국문화체험 등 여러 면에서 대성황을 이루었다. 특히 조직위는 이번 학술대회를 "풍성한 볼거리, 먹을거리를 제공하는 축제의 장"으로 만들고자 노력하였다. IEEE CASS President인 Thanos Stouraitis교수, 여러 IEEE CASS BoG와 ExCom 멤버를 비롯하여 국내외 많은 참석자로부터 역대 가장 성공적인 대회 중 하나라는"The Best Ever(역대 최고)" 찬사를 받았다. 이는 무엇보다도 국내 조직위원들의 헌신적인 노력과 학생들의 자발적 자원 봉사 등 여러 면에서 큰 역할을 했기 때문이다.

이번 학술대회에는 4번의 소셜 이벤트인, Welcome Reception, WiCAS(Woman in CAS) Banquet, Banquet, 국립박물관에서의 Farewell Party에 여러 다양한 행사를 준비하였다. 일요일 열린 전야제에는 처음으로 CASS 회원들로 구성된 CASSCODE Band 공연이 있었다. 그러나 드럼 주자인 이태리의 Massimo Alioto 교수가 여권을 분실하여 참여를 못해 드럼 주자를 급하게 국내에서 구했으나, 드럼 주자의 연주 실력이 출중하여 처음 구성된 밴드를 이끌어 주었고, 싱어는 필자를 포함, 여러 나라에서 참석 노래 실력을 뽐내었다. 특히 연주자, 가수들이 여러 나라에 흩어져 있어 리허설을 할 수 없어, 당일에만 리허설을 하였음에도 불구, 많은 박수를 받았다. 월요일 저녁에는 WiCAS(Woman in CAS) Event와 PhD/GoLD(Graduates of Last Decade) Event를 학술대회 사상 처음으로 합동개최, Panel Discussion 및 Networking Event에 500여 명이 참석 큰 호응을 얻었다.

화요일 뱅퀫에는 전북 국악원 단원 60여 명이 대규모로 참석하여, 기존 국악 공연과 달리 창의적 프로그램을 통해 한국의 문화를 마음껏 느낄 수 있는 전통문화를 선보였고 전 세계적으로 요청해온 한류 스타 공연에 부응하여 K-POP 아이돌 그룹인 포미닛(4MINUTE)이 열창하여 참가자들로부터 열정적 박수갈채를 받았고 참가자들이 오래도록 기억될 공연을 선물하였다. 뱅퀫에서의 포미닛 공연은 한국관광공사의 비용 지원으로 가능하였다. 마지막 날인 수요일에는 국립박물관에서 개최, 박물관 관람 후 마당에서 대형 비빔밥 만들기 체험을 포함한 퓨전 국악팀의 공연을 선보인 Farewell Party를 진행하여 모든 참여자가 한국의 문화와 전통을 흠뻑 맛보게 하였다. 풍부한 볼거리 및 먹거리를 제공해 참가자들의 기억에 오래 남을 수 있는 추억을 심어주었고 한국에 대한 이해와 인식을 한층 개선시키는 기회를 제공하였다.

행사 후 이제는 어깨가 많이 가벼워졌지만, 아직 그렇게 못 느끼는 것은 필자가 국내외 위원들과 참가자들, 특히 헌신과 열정을 쏟아 행사를 성공적으로 이끈 국내 위원분들께 진 크나큰 빚을 어떻게 갚아야 할지 고민이 되기 때문이다. 또한, 성공적 행사를 위해 최선을 다한 국내 위원님들의 헌신적 노력과 봉사를 잊을 수 없다. 저는 이번 행사를 통해 헌신, 조직력, 성공에 대한 열성을 가진 국내분들이 많음에 놀라움과 긍지를 느낀다.

지금도 2008년 5월 17일 유치 성공 소식을 들었을 때의 기쁨을 잊을 수가 없으며 유치 선정 회의에 같이 참여하였던 유치위원들께 진심으로 감사드린다. 또한, 성공적 개최를 위해 100여 번의 회의를 통해 성공적 개최를 이룬 조직위원들께 다시 한번 감사드린다. 과거부터 들어왔던 "한국민은 개개인은 훌륭하나, 단결이 안 되는 민족"이라는 말이 무색하게 사십여 분의 한국 위원들이 일심 단결하여 헌신적으로 노력하여 한 부분도 어긋남 없이 무결점 진행을 선보여 외국 참가자들에게 놀라움과 찬사를 받았다.

ISCAS 2012 개최는 최첨단 IT 산업의 국제교류 증대와 IT 기술 강국으로서 한국의 시스템 반도체 산업의 촉매제가 될 것으로 믿어 의심치 않는다. 이번 개최를 일회성으로 끝내지 않고, 앞으로도 이와 같은 국가적 행사를 유치 하여 IT 강국의 면모를 전 세계에 알릴 계기로 삼을 수 있으면 바람직하겠다. 찾아온 손님을 따뜻하게 환대하는 우리 민족의 오랜 전통처럼 학회 참가를 위해 우리나라를 방문한 외국의 반도체 회로 및 시스템분야 전문가들에게 감동을 선물하였고, 우리나라 관련 분야의 위상을 세계에 알릴 수 있는 ISCAS 2012가 되어 무엇보다 뿌듯하며, 나아가 국내 시스템 반도체 산업 발전의 촉매제가 될 것임을 믿어 의심치 않는다. 앞으로도 많은 분의 지도편달과 관심을 부탁드리며 다시 한번 성공적 학술대회 개최를 가능하게 해주신 모든 분의 후원과 배려에 머리 숙여 감사드린다.

아주대학교 전자공학부

선우명훈 교수
연구분야 : 멀티미디어 및 통신 SoC 설계, 저전력 설계
E-mail : sunwoo@ajou.ac.kr
http://soc.ajou.ac.kr