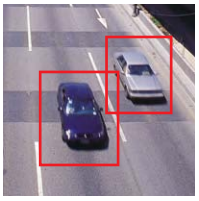
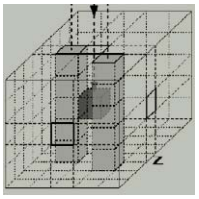




IDEC newsletter

Vol. 227 May 2016

기술동향칼럼1

자율주행의 핵심, 도로 위 여러 물체를 정확하게 실시간으로 인식하는 기술

지능형 차량을 위한 영상처리 및 비전 기술

기술동향칼럼2

SHA-1, 2를 넘어 보안 공격으로부터 정보를 안전하게 지킬 새로운 함수

차세대 암호학적 해쉬 알고리즘 SHA-3

기획칼럼1

높은 수준의 고성능 설계 지원을 제공한다

SILVACO사 Expert (EDA Tool 소개)

기획칼럼2

도래하는 IoT 시대에서 반도체의 역할을 다시 한번 상기하다

ISSCC 2016 후기

특집기사

상상이 현실로! '입는 컴퓨터'를 직접 제작한다

제12회 웨어러블 컴퓨터 경진대회

반도체설계교육센터
IC DESIGN EDUCATION CENTER

MPW/CDC

Multi-Project Wafer/Chip Design Contest

2016년 MPW 모집안내(5월)

- **모집일정** : 04.18(월)~05.02(월)
- **모집공정 및 회차** : MS350-1602회(우선)
  매그나칩 SK하이닉스 350nm 공정
- **참가대상** : IDEC 참여대학(Working Group)
- **신청방법** : IDEC 홈페이지(http://idec.or.kr)

MPW 진행일정 및 공정 지원내역

공정	회차구분 (공정_년도순서)	우선모집 (마감일)	정규모집 (마감일)	참여팀수/ 제작칩수	DB마감 (Tape-out)	Die-out	비고
삼성 65nm	S65-1601		2016.02.01	40 / 40	2016.08.01	2017.02.14	설계 대기중
	S65-1602		2016.04.18	13 / 40	2016.10.17	2017.05.02	설계 대기중
	S65-1603	2016.04.18	2016.06.20	6 / 40	2017.01.16	2017.07.31	정규모집 예정
MS 0.18um	MS180-1601		2016.01.18	33 / 25	2016.03.21	2016.08.22	제작중
	MS180-1602		2016.02.01	32 / 25	2016.05.16	2016.10.17	설계중
	MS180-1603		2016.03.07	25 / 25	2016.07.18	2016.12.19	설계중
	MS180-1604	2016.02.01	2016.04.04	26 / 25	2016.09.19	2017.02.20	설계중
	MS180-1605	2016.04.04	2016.06.07	12 / 25	2016.12.05	2017.05.08	정규모집 예정
MS 0.35um	MS350-1601		2016.02.01	20 / 20	2016.06.13	2016.10.04	설계중
	MS350-1602	2016.05.02	2016.07.04	- / 20	2017.01.16	2017.05.08	모집중(우선)

- 일정은 사정에 따라 다소 변경될 수 있음
- 회차 표기 방법 변경 : 공정코드-년도 모집순서 (예시) 삼성 65nm 2016년 1회차 : S65-1601)
- 모집 기간 : 모집 마감일로부터 2주 전부터 접수
- Package 제작은 Die out 이후 1개월 소요됨
- 내용 기준 : 2016.04.18

문의처
이의숙 | yslee@idec.or.kr, 042-350-4428
IDEC 홈페이지 | http://idec.or.kr

2016 IDEC SoC Congress Chip Design Contest (CDC) 개최 안내

- **일정 및 개최지**
  - 일정 : 2016년 6월 28일 또는 30일
    (미정-결정되는 대로 추후 안내 드리겠습니다.)
  - 개최지 : KAIST KI 빌딩
- **논문 접수 일정**
  - 논문 제출 기간 : 2016년 4월 8일 ~ 2016년 4월 29일
  - 선정 결과 안내 : 5월 16일
  - 일정은 사정에 의해 변경될 수 있습니다.
- **논문 참여 대상**
  - 2016년 1월 말까지 제작 완료된 설계팀 (해당 공정 및 회차 – 아래 표 참고)

D180-1404	MS180-1404	MS350-1402	S65-1402	TJB180-1402	TBC180-1402
D350-1404	MS180-1501	MS350-1501	S65-1403	TJB180-1501	TJR180-1402
	MS180-1502		S65-1501	TJB180-1502	
	MS180-1503				
	MS180-1504				

  - CDC 미참여팀 (개별 안내함)
- **논문 접수 방법**
  - 논문 작성 요령 : IDEC 논문 양식으로 제출, 영문 또는 한글로 1page 작성 (IDEC 홈페이지에서 다운로드 가능)
  - 논문 제출하기 : 반드시 IDEC 홈페이지에서 제출해 주셔야 합니다.

문의처
김하늘 | E. kimsky1230@idec.or.kr
T. 042-350-8535

교육프로그램 안내

2016년 5월

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

강좌 일정

센터명	강의일자	강의 제목	분류
본센터	5월 12~13일	Sentaurus TCAD Training	Tool강좌
	5월 19~20일	XMODEL과 Cell-Based Design Flow를 활용한 디지털 PLL 설계	설계강좌
	5월 23~25일	[IDEC 연구원 교육] Full-Custom 설계 Flow 교육	설계강좌
	5월 27일	CMOS 공정 및 마스크 레이아웃	설계강좌
한양대	5월 9일	오류정정 부호 기술 및 아키텍처 설계	설계강좌
	5월 11일	Brain-inspired Artificial Intelligence	설계강좌

본센터

5/12-13

강좌제목 Sentaurus TCAD Training
강 사 김명우 과장(Synopsys Korea)
강좌개요
Sentaurus TCAD의 기본적인 기능을 이용하여 TCAD simulation에 대한 이해를 높이고자 함.

수강대상 TCAD User(대학원생) **강의수준** 초급
강의형태 이론+실습 **사전지식 · 선수과목** CMOS 공정 및 소자 동작 원리

5/19-20

강좌제목
XMODEL과 Cell-Based Design Flow를 활용한 디지털 PLL 설계
강 사 김재하 교수(서울대학교)
강좌개요
본 강좌에서는 서울대학교 혼성신호 IC 및 시스템(MICS) 연구실에서 약 7년간 준비해 온 Cell-Based Flow를 활용한 아날로그/혼성신호 IC의 설계 기법을 선보입니다. 목표하는 바는 아날로그 IC도 디지털 IC처럼 behavioral language를 통해 그 동작을 기술하고, 모델 기반의 시뮬레이터를 통해 그 동작 및 성능을 확인하며, 셀라이브러리와 합성 툴, P&R 툴을 통해서 트랜지스터 수준의 회로에 대한 전문가적 이해 없이도 쉽게 IC의 layout 구현 및 tape-out이 가능한 flow를 완성하는 것입니다. MICS 연구실은 이러한 방법으로 설계한 우수한 성능의 디지털 PLL을 2016년 ISSCC학회에 발표한 바 있습니다.
특히, 본 강좌에서는 대표적인 혼성신호 시스템인 디지털 위상동기루프(phase-locked loop; PLL)에 초점을 맞추어, 참여하는 수강생들이 단 2일만에 디지털 PLL의 개념을 익히고, 스스로 설계한 디지털 루프 필터를 탑재한 자신만의 PLL을 설계하며, 제공되는 아날로그 셀라이브러리를 통해 바로 tape-out이 가능한 final GDS 형태의 DB를 완성할 수 있도록 진행할 예정입니다. 이를 위한 XMODEL 시뮬레이터, Design Compiler 합성 툴, IC Compiler P&R 툴을 포함한 각종 설계 및 검증 툴에 대한 사용법 및 효과적인 혼성신호 IC 설계를 위한 노하우를 공개할 것입니다.

수강대상 학부생, 대학원생, 직장인
강의수준 중급(아날로그 및 혼성신호 시스템 설계)
강의형태 이론+실습
사전지식 · 선수과목
- XMODEL을 활용한 아날로그 모델링 및 시뮬레이션의 기초
- Verilog를 활용한 디지털 모델링 및 시뮬레이션의 기초
- Feedback 제어시스템에 대한 기본적인 이해

5/23-25

강좌제목 [IDEC 연구원 강의] Full-Custom 설계 Flow 교육
강 사 조인신 연구원(IDEC)
강좌개요
CMOS 공정을 이용한 Full-custom 설계를 위한 기초 원리로서 설계 Flow에 대해 알아보고, 설계에 필요한 EDA Tools(Cadence Virtuoso, Mentor Calibre 등)의 설치 및 환경 설정 방법과 이 EDA Tools를 이용하여 실습 프로젝트를 수행함으로써 설계능력을 배양한다.

수강대상 CMOS 공정을 이용한 아날로그 설계 분야의 입문자 **강의수준** 초급
강의형태 이론+실습 **사전지식 · 선수과목** 전자회로, 반도체 공학, 회로이론

5/27

강좌제목 CMOS 공정 및 마스크 레이아웃
강 사 조성재 교수(가천대학교)
강좌개요
기본적인 반도체 소자인 pn 접합 다이오드와 MOSFET의 동작 원리, CMOS process의 단위 공정, CMOS inverter 제작을 위한 마스크 레이아웃과 process integration, 현대 VLSI 기술의 방향의 bottom-up 내용으로 진행한다.

수강대상 학부 4학년 및 대학원생, 관련산업 엔지니어 **강의수준** 초급
강의형태 이론 **사전지식 · 선수과목** 반도체소자(권장)

문 의 | KAIST IDEC 이한나 (042-350-8536, lhn1224@idec.or.kr)

한양대

5/9

강좌제목 오류정정 부호 기술 및 아키텍처 설계
강 사 이한호 교수(인하대학교)
강좌개요
오류정정 부호 기술은 전송단과 수신단 간의 통신에 따른 데이터의 오류를 검출 및 정정하고 최소화하여 데이터의 품질을 크게 개선할 수 있는 기술이다. 고성능 오류정정 기술로서는 BCH 부호, Reed-Solomon(RS) 부호, Turbo 부호, LDPC 부호 등이 있고 최근 Polar 부호 등이 많은 관심을 받고 있으며, 정보 손실을 최소화 할 수 있는 고성능 오류정정 부호 기술의 중요성이 증가하고 있다. 따라서, 다양한 응용시스템에 사용되고 있는 오류정정 알고리즘들을 소개하고 오류정정 알고리즘을 SoC 아키텍처로 구현하기 위한 설계 방법들을 소개한다.

수강대상 학생, 일반인 **강의수준** 초급 **강의형태** 이론

5/11

강좌제목 Brain-inspired Artificial Intelligence
강 사 이상완 교수(KAIST)
강좌개요
Recent advances in artificial intelligence(AI) research have paved the way for developing human-level intelligent systems. This begs the question of how the human brain handles a wide variety of tasks, whereas AI systems need to function in a task-specific way. This talk puts together ideas from nascent fields of AI and neuroscience to appreciate the human brain's ability that cutting-edge AI lacks. I will provide a brief overview of the brain-inspired AI approach, and then present evidence suggesting that [1] the brain consists of multiple subsystems for hierarchical abstraction that translates external inputs into internal codes to produce compact representations for learning and inference and [2] implemented in the human prefrontal cortex is the hierarchical cognitive control mechanism, allocating control over behavior to brain's subsystems in a way that is optimal for the agent under various constraints.

수강대상 학생, 일반인 **강의수준** 초급 **강의형태** 이론

문 의 | 한양대 IDEC 오경주 (031-400-4079, ipc@hanyang.ac.kr)

기술동향1

지능형 차량을 위한 영상처리 및 비전 기술

신현철, 박경춘, 범설, 이르판 리아즈, 야와르 레흐만 | 한양대학교

서론

최근 차량에 장착한 센서를 이용하여, 차량, 보행자, 교통 표지판, 차선 등 주행 관련 외부 환경에 대한 데이터를 수집하여 인지하는 첨단 운전자 보조시스템(Advanced Driver Assistance Systems: ADAS)에 대한 연구가 활발히 진행되고 있으며, 이는 다음 단계인 무인 운전 기술의 핵심 부분이다.

지능형 차량 기술은 안전하고 편안한 운행과 환경 보호에 기여할 수 있다. 교통사고의 약 94%는 운전자 과실로 인해 발생한다. 세계보건기구는 전 세계 자동차 사고 사망자가 매년 120만명에 이른다고 발표하였다. 2015년 1월 모건 스텐리는 무인 자동차가 교통사고를 감소시켜 전 세계적으로 연간 5조 6000억달러의 비용 절감 효과를 가져올 수 있다고 추정하였다. 교통사고 절감 뿐만 아니라 자동차의 운행 효율을 개선하여 에너지 소비 감소 및 환경 오염 감소 또한 가능할 것으로 예상한다.

단순한 무선 송수신을 이용한 무인 차가 1925년에 선보여진 이후, 2020년에 무인 자동차의 상용화를 발표한 구글에 이르기까지 무인 자동차 개발은 계속되고 있다. 미국 도로교통안전국은 그림 1과 같이 차량의 자동화 수준을 기술 정도에 따라 0단계부터 4단계까지 총 5개 단계로 구분하였다. 현재 글로벌 차량 제조사들과 ICT 기업들은 2단계와 3단계 기술을 상품화하고 4단계를 위한 기술을 경쟁적으로 개발하고 있다.

단계	내용
0단계 (No-Automation)	운전자가 차량을 항상 조종
1단계 (Function-specific Automation)	자동 브레이크 등 단일 기술자동화
2단계 (Combined Function Automation)	크루즈 기능과 차선 유지기능 등 2가지 이상 기술의 융합
3단계 (Limited Self-Driving Automation)	고속도로 등 특정 조건하에서의 자율주행
4단계 (Full Self-Driving Automation)	모든 상황에서 완전한 자율 주행

그림 1. 차량 자동화 수준의 단계

시장 조사 기관들은 2020년대에 자율주행 자동차 시장 형성이 본격화 될 것으로 전망하고 있다. 그림 2에서는 무인 자동차의 판매량 및 시장 전망을 보여준다. 보스턴컨설팅그룹은 무인 자동차 시장 규모가 2025년에 약 420억 달러에 이를 것이며, 2035년이 되면 770억 달러 규모로 성장할 것으로 예상하였다. IHS 오토모티브에서는 2035년에 무인 자동차의 판매량이 1,000만대를 넘어 자동차 시장의 약 10%를 차지할 것으로 예측하였다.

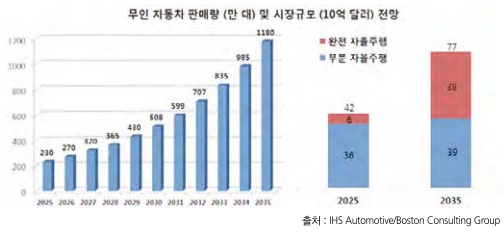


그림 2. 무인 자동차 시장규모 및 전망

이에 운전자를 돕거나 자율주행에 활용할 수 있는 다음과 같은 기술들을 소개한다. 먼저 영상에서 안개 영향을 제거하여 영상 신호를 보정하는 기술을 알아보고, 이어서 차선과 도로 상황 인식에 필요한 도로 소실점 검출 기술 및 차량 운행에 중요한 정보인 비전 기반 보행자/차량 인식 기술에 대하여 알아보도록 한다.

최근 기술 동향

ADAS는 기존 기계 부품 외 센서와 레이더 등 다양한 전자 장비로 수집한 데이터로 자동차를 제어한다. 그 중에서도 가성비가 높은 카메라 센서를 이용하는 비전 기반 영상 처리 및 인식 기술들이 핵심이라고 할 수 있다. 영상에서 안개 영향으로 인한 노이즈 제거 기술, 도로 환경을 인식하기 위한 도로 소실점 검출 기술, 차량/보행자 등 도로 주변 인프라를 인식하는 기술은 자율주행에 필수적인 기술이며, 현재까지 아래와 같은 관련 방법들이 제안되었다.

1. 안개 영향 제거(De-hazing)

- 영상에서 안개의 영향을 제거하기 위한 기술로 단일 영상에 기반한 기술과 추가 정보를 이용한 기술로 분류할 수 있다.
- 추가 정보는 다른 조건에서 얻은 여러 장의 영상을 이용하거나, 적외선 영상 또는 거리지도(depth map)를 이용하는데, 이러한 정보가 없을 때에는 사용할 수 없다는 단점이 있다.
- 단일 영상을 이용하는 방법은 통계적인 가정을 사용하는데, 예를 들어 partially un-correlated transmission, target surface shading, dark channel prior 등을 사용한다[1-3]. 단점으로는 하늘처럼 밝은 부분, 야간 안개, 조명이 불균일할 때, 성능이 떨어지며 실시간 처리가 어렵다는 점이다.

2. 도로 소실점 검출(Road Vanishing Point Detection)

- 소실점 검출 방법은 edge 기반 방법과 texture 기반 방법으로 분류할 수 있다.
- Pixel 기반 방법은 속도 또는 정확도 면에서 좋지 않다.
- 에지(edge) 기반 방법은 Hough transform[4] 과 함께 관심 영역(Region of Interest) 탐색, Principal component analysis 기술 등을 사용하는데[5], 도로 경계가 분명한 영상에서는 잘 동작하지만 산악 또는 사막 지역 등 도로 경계가 분명하지 않은 경우에는 정확도가 크게 떨어진다.
- 텍스쳐(texture) 기반 방법은 Gabor filtering와 soft voting 기술을 사용하거나 adaptive distance based voting 기술을 사용하는데, 포장 도로는 물론 un-structure road에서도 비교적 잘 동작한다. 배경에 의한 noise를 줄이고, 계산 속도 면에서 효율적인 새로운 방법 개발이 필요하다.

3. 보행자 인식

- 보행자 인식은 많은 연구가 진행된 분야이며, 우리 연구실에서도 상당한 기술을 확보하고 있는데, 다양한 pose, 의상, occlusion 등으로 인하여 인식에 어려움이 있다.
- Haar like features, Histogram of Oriented Gradients(HOG), deformable part model, aggregated channel features 등의 방법이 사용된다[6-7].

■ 앞으로 pose variation과 occlusion을 잘 처리하기 위한 연구가 필요하다.

4. 차량 인식

■ 안전한 주행을 위해서는 주변의 차량을 인식해야 한다.

■ 카메라 영상으로부터의 차량인식 기술로는 part-based model, constellation model, implicit shape model 등이 개발되었다[8-10].

■ 거리가 먼 차량 또는 일부 가려진 차량의 인식 기술을 개선할 필요가 있다.

창의적인 기술 제안

1. 안개 영향 제거(De-hazing)

■ 기존의 dark channel prior 방법의 결점을 보안하기 위하여 새로운 block-to-pixel interpolation 방법을 제안하였다[11]. 제안한 방법의 흐름도는 아래의 그림 3과 같다.

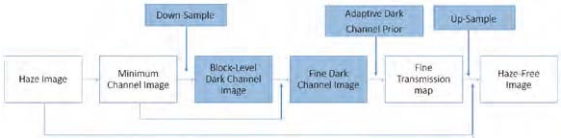


그림 3. 제안한 도로 소실점 검출 기술의 흐름도

■ Transmission map 생성 과정의 효율적성을 높이기 위하여 block-to-pixel interpolation 방법을 이용하여 픽셀 레벨과 블록 레벨의 dark channel을 결합한다.

■ 기존의 dark channel prior이 영상의 하늘 부분에서의 제한성을 보완하고자, 가우시안 커브를 이용한 adaptive dark channel prior을 제안하여 하늘 부분과 조도가 높은 부분에서 보다 자연스럽게 영상을 보정한다.

■ 제안한 방법의 보정 성능은 기존 최첨단 수준의 기술보다 우수하며, 효율성도 기존 방법의 30배이다. 그림 4에서는 기존 방법과의 결과 비교를 보여준다.

그림 4. 기존 방법과 제안한 방법의 SSIM(Structural Similarity) 비교 (높을수록 성능 우수)

2. 도로 소실점 검출(Road Vanishing Point Detection)

■ 제안한 소실점 검출(vanishing print detection) 방법의 주요 흐름 도는 아래 그림과 같다.

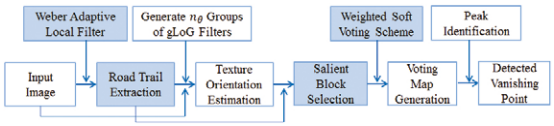


그림 5. 제안한 도롤 소실점 검출 기술의 흐름도

■ 도로 소실점을 검출할 때 도로 영상의 모드 픽셀이 유용한 것이 아니고, 그 중에서 도로의 자국 또는 경계에 해당하는 픽셀들만이 유용한 voting에 기여한다.

■ Weber local descriptor(WLD)의 differential excitation component는 texture와 배경을 분리하는데 용이하기에, 이런 아이디어에 기반하여 도로 자국과 배경을 구분하는 Weber adaptive local filter을 제안하였다.

■ 도로 자국의 정확하지 않은 texture orientation으로 인한 noise votes를 제거하고 검출을 가속하기 위하여, salient-block-wise weighted soft voting를 제안하였다.

그림 6. 제안한 방법과 기존 방법의 결과 비교

■ 위의 그림 6에서 초록색 점은 ground truth이고, 빨간 색은 제안한 방법의 결과이며, 나머지는 최근 발표된 기술의 결과이다. 비교를 거쳐 얻은 결과, 제안한 방법의 평균 인식률은 3.6% 향상되었고, 기존 방법보다 10배 빠르다.

3. 보행자 인식

■ 우선 최첨단 기술인 Aggregate Channel Features(ACF)를 사용하여 보행자 후보 지역을 생성한다.

■ Discriminative patch를 이용하여 후보 영상을 여러 개의 random patch로 분할하여 따로 특징을 추출하고, Support Vector Machine를 통하여 분류된 negative patch의 개수를 통하여 최종적으로 보행자를 검출한다. 제안한 방법의 흐름도는 아래 그림 7과 같다.

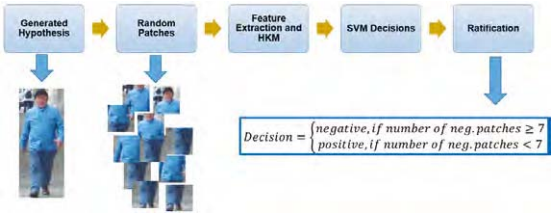


그림 7. 제안한 discriminative patch 기반 방법의 흐름도

■ 제안한 방법은 일반 상황에서의 보행자 인식 성능을 향상 시킬 뿐만 아니라, 일부만 보이는 상황에서도 보행자를 효과적으로 검출한다.

4. 차량 인식

■ Occlusion hypothesis를 확인하기 위하여 geometric과 likelihood를 활용하여 가려진 차량을 검출하는 기술을 개발하였다.

■ UIUC 차량 benchmark dataset를 기준으로 우리가 제안한 방법의 인식률은 기존의 최우수 기술인 Hough forest 기반 방법의 인식률과 비슷한 수준(98~99%)이다.

그림 8. 기존 Hough forest 기반차량인식 방법(a, c, e)과 제안한 방법(b, d, f)의 결과 비교

■ 위의 그림 8에서는 제안한 차량인식 방법과 기존 Hough fores 방법의 결과 비교를 보여준다.

기술동향1

실시간 동작

비전 기반 운전자보조시스템은 차량 주행의 특성상 정확해야 할 뿐만 아니라, 처리 속도가 충분히 빨라서, 모든 영상 처리 및 인식 기술이 통합된 시스템은 실시간으로 동작 가능해야 한다. 100km로 주행하는 차량은 1초에 약 28m를 이동한다. 시스템의 효율성을 높이려면 처리 및 인식 성능을 유지하는 동시에 알고리즘의 복잡도를 줄여 수행 시간을 최적화해야 하고, 병렬처리가 가능한 고속처리 하드웨어도 활용해야 한다.

1. 알고리즘 최적화

- **안개 영향 제거** : 고 해상도 영상을 실시간으로 처리하기 위하여, 효율적인 down-scaling 방법을 제안한다. 우선 입력영상을 down-scale하여 복잡도가 높은 부분에서 사용하여 transmission map을 얻은 후, de-hazing 처리 후에 다시 up-scale하여 안개 영향이 제거된 영상을 얻음으로써 수행시간을 단축한다.
- **도로 소실점 검출** : 현재 수행 시간이 가장 많이 소요되는 부분은 매 픽셀을 후보로 삼는 voting 과정이다. 이 문제를 해결하기 위하여 horizon line과 확률이 높은 관심 영역을 미리 설정하는 방법을 이용하여 수행시간을 줄여서 효율을 높인다.
- **보행자/차량 인식** : 영상에서 논리적으로 관심 영역을 설정함으로써, 차량과 보행자를 탐색하는 영역을 줄인다. 또한 인식률을 보장하는 전제하에서 물체를 검출에 필요한 pyramid scale의 계층 수를 줄인다.

2. 병렬처리 가능한 하드웨어 사용

- 소개한 세 가지 기술은 전부 스펙이 Intel i7-3770 3.4GHz(dual core) CPU &8GB RAM인 컴퓨터에서 MATLAB 기반으로 구현되었기에 실시간 동작이 어렵다. 알고리즘의 최적화도 중요하지만 설계한 알고리즘을 GPU, 임베디드 시스템 및 ASIC 등 병렬처리가 가능한 하드웨어로 구현하여 실시간 동작이 가능하도록 한다.

결론

최근 지능형 차량 관련 연구가 세계적으로 활발하게 진행되고 있으며, 핵심 기술의 하나인 지능형 차량을 위한 비전 기술도 상당한 발전을 보이고 있다. 하지만, 안전하고 편리한 주행을 지원하거나 자율주행을 하기 위해서는 아직 해결해야 할 기술적인 문제가 많다. 창의적인 연구가 필요한 부분은 다양한 날씨(안개, 비, 눈), 환경(역광, 터널, 지하) 및 상황(다양한 색상/모양, 일부 가려짐)에서 정확하게 실시간으로 도로 상의 여러 가지 물체를 인식할 수 있는 기술을 개발하는 것이다.

참고문헌

1 R. T. Tan, "Visibility in bad weather from a single image," CVPR, 2008, pp. 1-8.

2 T. Ketan, et al., "Investigating Haze-Relevant Features in a Learning Framework for Image Dehazing," CVPR, 2014, pp. 2995-3002.

3 Y. Wang, et al., "Single Image Defogging by Multiscale Depth Fusion," IEEE Trans. Image Process., 2014. 23, pp. 4826-4837.

4 Nieto, M., Salgado, L.: 'Real-time vanishing point estimation in road sequences using adaptive steerable filter banks'. Proc. Int. Conf. Advanced Concepts for Intelligent Vision Systems, Glenelg, Australia, April 2007, pp. 840–848

5 Kong, H., Audibert, J.Y., Ponce, J.: 'General road detection from a single image', IEEE Trans. Image Process., 19, (8), 2010, pp. 2211–2220

6 P. Viola, M. Jones, and D. Snow, "Detecting Pedestrians Using Patterns of Motion and Appearance," International Journal of Computer Vision (IJCV), 2005.

7 N. Dalal and B. Triggs, "Histograms of Oriented Gradients for Human Detection," IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2005.

8 Felzenszwalb, P.F., Girshick, R.B., McAllester, D., Ramanan, D.:'Object detection with discriminatively trained part-based models', IEEE Trans. Pattern Anal. Mach. Intell., 2010, 32, (9), pp. 1627–1645

9 Leibe, B., Leonardis, A., Schiele, B.: 'Robust object detection with interleaved categorization and segmentation', Int. J. Comput. Vis., 2008, 77, (1-3), pp. 259–289

10 Gall, J., Yao, A., Razavi, N., Van Gool, L., Lempitsky, V.: 'Hough forests for object detection, tracking, and action recognition', IEEE Trans. Pattern Anal. Mach. Intell., 2011, 33, (11), pp. 2188–2202

11 Y. Teng, et al., "Real-time single image dehazing using block-to-pixel interpolation and adaptive dark channel prior," IET Image Process., 2015. 9, pp. 725-734.

저자정보

신 현 철 | 한양대학교 전자공학부
연구분야
System on Chip (SoC) Design Methodology and CAD software development
Image processing and computer vision for Intelligent vehicle
E-mail shin@hanyang.ac.kr
Homepage digital.hanyang.ac.kr

박 경 춘 | 한양대학교 전자통신공학과
연구분야
Image processing and computer vision for ADAS
Lane detection / Image de-weathering / Image stitching
E-mail kcpark@digital.hanyang.ac.kr

범 설 | 한양대학교 전자통신공학과
연구분야
Image processing / Computer vision / Pattern recognition
E-mail fanxue@digital.hanyang.ac.kr

이르판 리아즈 | 한양대학교 전자통신공학과
연구분야
Image processing and computer vision for ADAS
Image de-weathering
E-mail irfancra@gmail.com

야와르 레흐만 | 한양대학교 전자통신공학과
연구분야
Object detection and recognition
Image processing / Class specific ROI detection
E-mail rehman_yawar@yahoo.com

기술동향2

차세대 암호학적 해쉬 알고리즘 SHA-3

최병윤 교수 | 동의대학교 컴퓨터공학과

머리말

정보 보호 분야에서 암호화 알고리즘만큼 중요하다고 평가되는 암호학적 해쉬 알고리즘(cryptographic hash function)은 통신 정보와 저장 매체에 담긴 정보의 위·변조 여부를 확인하는 기술이다. 네트워크 등에서 전송 오류 발생을 확인하기 위해 사용하는 순환 중복 검사(CRC, cyclic redundancy check) 혹은 체크섬(checksum) 알고리즘도 해쉬 함수 특성을 갖고 있지만, 악의적인 공격자에 의한 의도적인 정보 변조를 검출하지 못하는 한계가 있다. 암호 분야의 경우 정보를 안전하게 지키는 것이 목적이므로 암호학적 해쉬 알고리즘은 악의적인 공격자에 의한 능동적 공격에 대처할 수 있어야 하므로 더 강력한 보안 특성을 갖추고 있어야 한다[1-2].

암호학적 해쉬 알고리즘은 공개키 암호 알고리즘인 RSA의 공동 개발자인 MIT 공과대학의 Rivest 교수가 만든 MD4, MD5와 Secure Hash Algorithm(SHA) 알고리즘이 90년대부터 널리 사용되고 있으며, 각국은 보안 문제로 독자 암호학적 해쉬 알고리즘을 개발하고 있다. SHA는 MD4를 기반으로 미국 표준 기술 연구소(NIST, National Institute of Standards and Technology)에서 개발하였고, 1993년에 FIPS(Federal Information Processing Standard) PUB 180으로 공표되었다. 현재는 SHA-0로 알려진 SHA는 취약점이 발견되어 1995년에 160비트 길이를 갖는 해쉬 값을 사용하는 개정된 버전(SHA-1)이 FIPS PUB 180-1로 발행되었다. 2002년에 NIST는 SHA-1을 수정하여 4개의 해쉬 출력 길이(224, 256, 384, 512 비트)를 갖는 새로운 표준(SHA-2) FIPS 180-2를 발표하였다. 그런데 기존에 알려진 280보다 훨씬 적은 269의 연산 횟수로 두 개의 별도의 메시지로부터 동일한 SHA-1 해쉬 값을 생성하는 공격 방안이 발표되었다[3]. 이에 NIST는 512-비트 해쉬 출력을 갖는 SHA2-512 방식은 거의 난공불락으로 알려져 있었지만, SHA-1, MD5와 동일한 구조와 수학적인 연산에 바탕을 두고 있어 SHA-2가 위험해지는 경우를 대비하여 이들 대신할 수 있는 차세대 해쉬함수 SHA-3을 제정하기로 하였다[4]. NIST는 1997년에 미국 표준 대칭키 암호 알고리즘인 DES(Data Encryption Standard)를 대신하는 AES(Advanced Encryption Standard)를 제정할 때 공개적인 방식을 통해 후보를 모집한 다음 함수 안전성을 분석하여 몇 차례에 걸쳐 후보를 걸러내는 방식으로 진행한 바 있다. NIST는 SHA-3에도 동일한 방식을 적용하여, 2007년 SHA-3에 대한 요구 조건을 공개하여, 전 세계 암호 연구 기관으로부터 해쉬 알고리즘을 접수받은 후, 5년 간 3 라운드에 걸친 평가 과정을 거쳐서 2012년 10월 이탈리아와 벨기에 연구팀이 공동으로 개발한 Keccak을 SHA-3(PUB 202)로 선정하였다. NIST는 선정한 Keccak에 표준화 과정을 거쳐 2015년 8월 최종 문서가 발간되었다[5]. SHA-3 알고리즘은 고정된 위치 교환(permutation)에 바탕을 둔 새로운 스폰지 함수(sponge function)를 사용하며, 매개 변수에 따라 성능과 암호 강도를 적절히 조절할 수 있고 가변 길이의 해쉬 출력을 생성할 수 있다.

본 원고에서는 암호학적 해쉬 함수의 특성과 동작 원리를 살펴본 후, SHA-3의 세부적인 동작을 다루고, 마지막으로 SHA-3의 구현 방안과 향후 전망을 살펴본다.

암호학적 해쉬 함수의 특성

해쉬 함수 H()는 가변 길이 데이터 M을 입력으로 받아서, 고정 길이의 해쉬 값 $h=H(M)$을 생성한다. 여기서 M은 해쉬 값 h의 선이미지(preimage)라 하며, 해쉬 함수 H()는 다대일 대응 특성을 갖고 있으므로 동일한 해쉬 값 h를 갖는 여러 개의 선이미지가 존재하는 충돌(collision) 상황이 발생할 수 있다. 보안 응용에 필요한 해쉬 함수는 암호학적 해쉬 함수라 하며 표 1과 같은 특성을 갖고 있어야 한다.

표 1. 암호학적 해쉬 함수 $H()$의 성능 특성

항 목	설 명
가변 길이 입력	H()는 어떤 길이의 입력 메시지도 처리 가능해야 함
고정된 출력 길이	H()는 고정 길이의 출력을 가져야 함
효율성	H(M)은 하드웨어와 소프트웨어에 적용하기 용이해야 하며, 어떠한 메시지에 대해서도 계산이 비교적 수월해야 함
일방향성 (선이미지 회피성)	어떠한 해쉬 값 h에 대에서도 인 M을 찾는 것이 계산적으로 어려움
약 충돌 회피성 (2차 선이미지 회피성)	어떤 메시지 M_1에 대한 해쉬 값 h이 주어졌을 때 $(h=H(M_1))$, 그 해쉬 값 h를 갖는 다른 입력 메시지 M_2를 발견해내는 것이 계산상 어려워야 함
충돌 회피성 (강한 충돌 회피성)	동일한 해쉬 값$(H(M_1)=H(M_2))$을 갖는 2개의 다른 메시지, M_1과 M_2짝을 찾는 것이 계산적으로 불가능해야 함
의사 난수성	$H()$의 출력이 의사난수에 대한 표준 시험을 만족해야 함

그림 1은 가변 길이 입력과 고정 길이 출력을 처리하는 Merkle-Damgard 해쉬 함수 구성 기법을 나타낸다. 가변 길이의 메시지를 동일한 길이의 블록으로 나눈 후 일방향 압축 함수, $f()$를 반복적으로 적용한다. 각 $f()$ 함수의 입력은 이전 $f()$함수의 결과와 메시지 블록이 사용되는데, 첫 번째 입력으로 미리 정의된 초기 상수 IV가 사용된다. 단 입력 메시지 M이 $f()$ 함수에 처리에 필요한 블록 길이의 배수가 되도록 마지막 블록은 길이 정보를 포함한 적절한 패딩 처리가 필요하다.

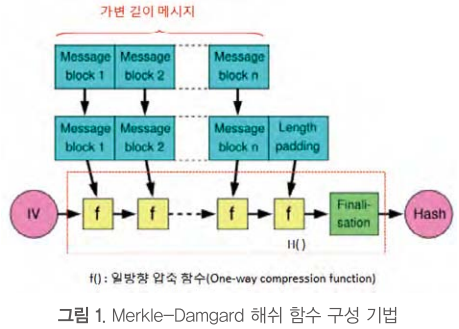


그림 1. Merkle-Damgard 해쉬 함수 구성 기법

기술동향2

스폰지 함수

SHA-3 해쉬 알고리즘은 스폰지 함수에 기반을 두고 있다. 스폰지 함수 $f()$는 기존 반복 구조의 해쉬 함수와 유사하게 입력 메시지를 고정된 크기의 블록으로 나누고, 각 블록은 차례로 처리되며, 각 반복 함수의 결과는 다음 반복 구조에 입력되어 최종 출력을 생성한다. 이러한 스폰지 함수가 기존 해쉬 함수와 다른 점은 가변 길이의 입력과 함께 가변적인 출력 길이를 제공할 수 있어서, 고정된 길이의 해쉬 함수 응용과 함께 고정 길이 입력에 대해 가변 길이 출력을 생성하는 의사 난수 생성기에도 응용이 가능하다. 그림 2는 가변 길이 입력 메시지 M를 받아서 가변 길이 출력 Z를 생성하는 스폰지 함수 동작을 나타낸다. 스폰지 함수(Z=sponge[f, pad, r](M, n))는 4개의 주요 매개변수로 정의된다. 여기서 $f()$는 각 블록을 처리하는 내부 함수, r은 입력 블록의 크기, pad는 패딩 알고리즘, n은 출력의 길이를 나타낸다.

스폰지 함수는 가변 길이 입력과 가변 길이 출력을 지원하기 위해 정보 흡수 단계(absorbing phase)와 출력 짜내기(squeezing) 단계로 나누어진다. 스폰지 함수는 b=r+c 비트인 상태 변수 s에 의해 동작하는데, 초기 상태 변수는 0으로 초기화되며, 각각의 반복 동작 시 새로운 값으로 갱신된다. r-비트는 입력 메시지를 분할하는 블록 크기로 블록 크기가 클수록 스폰지 함수가 처리하는 메시지의 비트율(bit rate)이 증가한다. c는 용량(capacity)이라 불리며, 스폰지 함수가 얻을 수 있는 보안 수준을 결정한다. b값이 고정인 경우 c 비트가 증가할수록(r-비트 길이 감소), 보안 수준은 증가하고 처리 성능은 떨어지며, c 비트가 감소할수록 보안 수준은 감소하지만 처리 성능은 증가한다. SHA-3에서 성능과 보안을 위해 권고하는 기본적인 비트 길이 값은 c=1024-bit, r=576-bit, b=r+c=600-bit이다. 가변 길이인 m-비트 입력 메시지는 블록 크기 r의 정수배가 되도록 패딩(채움 처리)이 되어, P_0, P_1, ..., P_k의 블록을 생성한다. 패딩 방식은 표준안에 상세하게 기술되어 있다. 각 P_i블록은 하위에 c개의 0을 추가하며, 이전 상태 값과 비트 단위의 XOR 연산을 한 후 $f()$ 함수를 거친다. f 함수의 결과는 다음 반복 동작의 입력 상태가 된다. 이러한 반복 동작은 메시지의 모든 블록이 소진될 때까지 반복되는데, 이러한 동작을 흡수 단계라 한다. 이러한 흡수 단계는 가변 길이의 입력을 처리하여 고정 길이의 b-비트 상태 출력을 생성하는 방안을 제공한다.

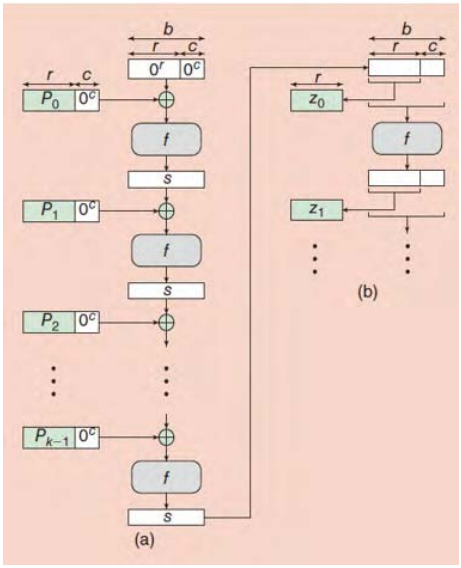


그림 2. 스폰지 함수 동작[6]
(a) 정보 흡수 단계(absorbing phase) (b) 정보 짜내기(squeezing phase) 단계

해쉬 함수의 원하는 출력 길이 n-비트가 블록 길이 r-비트보다 작거나 같을 경우($n \le r$), 흡수 동작 단계의 출력의 상위 n-비트에서 결과를 취하며, 출력 짜내기(squeezing) 동작 단계는 필요 없게 된다. 그러나 해쉬 함수의 원하는 출력 길이 n-비트가 블록 길이 r-비트보다 큰 경우 출력 짜내기 단계(그림 2(b))를 수행해야 한다. 먼저 흡수 단계의 출력 s-비트 중 상위 r-비트가 Z_0가 되며 원하는 출력 결과의 상위 r-비트를 구성한다. 그리고 나서 흡수 단계의 결과인 s-비트의 출력은 반복 함수 f()에 입력된다. 단 짜내기 과정에서는 흡수 단계의 반복 동작과 다른 점은 입력부의 XOR 처리가 없다는 점이다. 각 반복 동작마다 s-비트 결과의 상위 r-비트는 Z_{j-1} 블록으로 추출되어 이전에 생성된 Z_{j-2}블록에 연결된다. 이러한 과정은 원하는 길이의 출력이 생성될 때까지 반복된다. 현재 SHA-3의 표준안의 경우 최대 해쉬 출력 길이가 n=512로, 항상 r-비트보다 작으므로 흡수 단계의 결과만으로 원하는 길이의 해쉬 출력을 제공할 수 있어서 출력 짜내기 동작이 필요하지 않다. 이러한 출력 짜내기 동작은 반복 동작을 통해 원하는 다양한 가변 길이의 출력을 생성할 수 있으므로 길이 r-비트의 짧은 메시지를 종자(seed)로 사용하여 가변 길이의 난수를 생성하는 의사 난수 생성기로 활용 가능하다.

SHA-3 알고리즘

표 2는 SHA-3 표준 알고리즘에서 해쉬 출력 길이 n과 r, c, s의 길이 관계를 나타낸다. 표준안에서 상태 s의 길이는 1600 비트로 고정이지만, 해쉬 출력 n의 길이가 증가할수록 r을 작게 하고 c를 길게 하여 보안 수준을 향상시킨다. 여기서 주목할 특이사항은 용량 c가 출력 길이의 2배의 값으로 설정되었다는 점이다.

표 2. 해쉬 출력 길이 n과 블록크기(r), 용량(capacity, c), 상태(s) 사이의 길이 관계

SHA-3 알고리즘	해쉬 출력 길이(n) (비트)	블록 길이(r) (비트)	용량, c (비트)	상태 길이(s) (비트)
SHA3-224	224	1152	448	1600
SHA3-256	256	1088	512	1600
SHA3-384	384	832	768	1600
SHA3-512	512	576	1024	1600

SHA-3의 반복 함수인 $f()$ 함수는 입력으로 1600-비트의 상태 변수를 받아서, 5개의 세부 단계로 구성된 24 라운드로 구현된다. 그림 3은 SHA-3의 반복함수 $f()$를 나타낸다. 이러한 반복함수는 각각 메시지 블록을 처리하는데 사용된다.

$f()$ 함수의 각 단계는 단순한 위치 교환(permutation)과 대체(substitution) 동작으로 구성된 구조를 갖고 있어서 백 도어(trap door)가 숨겨질 수 없는 구조를 갖고 있다. SHA-3의 반복함수는 1차원 1600-비트 상태 변수 s대신에 그림 4와 같이 3차원 배열 구조로 동작 설명이 용이하다. 표준안에서 z축의 값은

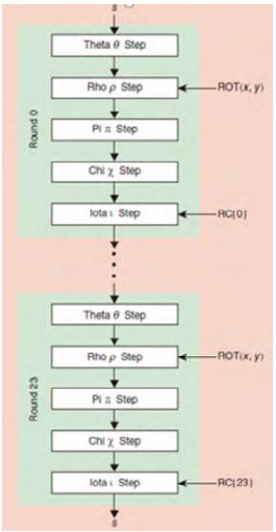


그림 3. SHA-3의 반복함수[6]

w-비트로 레인(lane) 으로 불리며, 상태 변수 s와 사이의 비트 대응관계는 식 (1)로 정의된다.

$$s[64(5y+x)+z] = A[x,y,z] \quad (1)$$

여기서, $0 \le x \le 4,\ 0 \le y \le 4,\ 0 \le z < w\ (w = 64)$

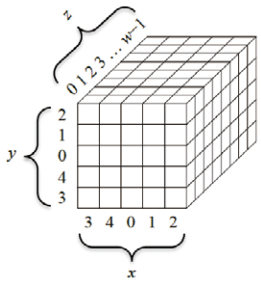


그림 4. 상태 S 변수의 3차원 배열 $A[x,y,z]$로의 매핑[5] (표준안의 W=64)

반복함수 $f()$의 첫 단계인 θ단계는 식 (2)로 정의된다. 여기서 $\sum$은 열(column)에 있는 모든 비트의 XOR 합을 나타낸다.

$$\theta : A[x,y,z] \leftarrow A[x,y,z] \oplus (\sum_{y'=0}^{4} A[(x-1) \bmod 5, y', z]) \quad (2)$$
$$\oplus (\sum_{y'=0}^{4} A[(x+1) \bmod 5, y', (z-1) \bmod 64])$$

θ 단계는 상태내의 각 비트를 3차원 배열 내 2개의 인접 열과의 XOR 동작을 나타낸다. 다음 상태의 각 비트는 현재 비트와 인접한 2개의 열의 10개의 비트로 구성된 총 11개 비트의 조합으로 결정된다. 이러한 동작은 중요한 보안 특성인 확산(diffusion) 특성을 구현한다. 그림 5는 θ단계 동작에서 하나의 상태 비트를 계산하는 동작을 나타낸다.

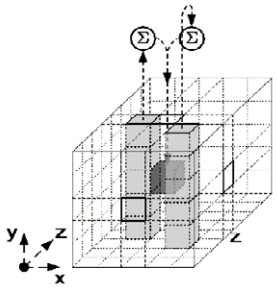


그림 5. θ 단계 동작에서 하나의 다음 상태 비트를 계산하는 동작[5]

두 번째 단계인 ρ단계는 다음과 같이 정의된다.

① x=y=0인 경우
$\rho : A[x,y,z] \leftarrow A[x,y,z]$

② x=y=0이 아닌 경우
(x, y)=(1, 0)
for t=0 to 23
{
$A[x,y,z] \leftarrow A[x, y, (z - \frac{(t+1)(t+2)}{2}) \bmod 64]$
$(x,y) \leftarrow (y, (2x+3y) \bmod 5)$
}

ρ단계는 레인 L(0,0)의 64-비트는 영향을 받지 않고, 다른 레인은 레인 내에서 회전 이동 동작을 한다. 변수 $0 \le t < 24$은 L(0,0)을 제외한 특정 레인 L(x,y)에 적용되는 회전 이동의 거리 $_{g(t)} = \frac{(t+1)(t+2)}{2}$를 결정한다. ρ단계에서 모든 레인에 적용되는 회전 이동 거리가 달라서 레인내 확산 효과를 구현한다.

π 단계는 고정된 z를 나타내는 슬라이스 간에 비트 이동을 나타내며 식 (3)으로 정의된다.

$$\pi : A[x,y,z] \leftarrow A[(x+3y) \bmod 5, x, z] \quad (3)$$

π 단계 동작은 5x5 행렬인 슬라이스 내에서 레인 간에 위치를 재배치하는 효과를 구현하며 그림 6은 π 단계의 동작 예를 나타낸다.

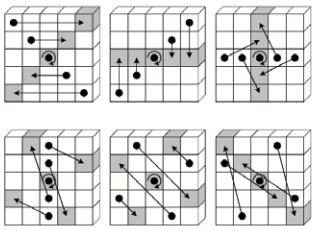


그림 6. 하나의 슬라이스(고정된 z 값)에서 π 단계 동작 예[5]

$$\chi : A[x,y,z] \leftarrow A[x,y,z] \oplus \quad (4)$$
$$((A[(x+1) \bmod 5, y, z] \oplus 1) \cdot A[(x+2) \bmod 5, y, z])$$

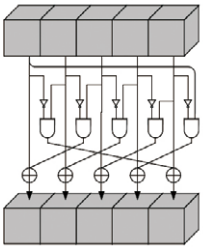


그림 7. 하나의 행에 적용되는 x단계 동작[5]

마지막 ι단계는 식(5)와 같이 라운드(i_r) 별로 다른 64-비트 라운드 상수(RC)와 레인 $L[0,0]$간의 XOR 동작으로 $L[0,0]$를 갱신한다. 64-비트 라운드 상수 RC[0,0,z]중 7-비트만 linear feedback shift register(LFSR) $rc[t]$로 결정되고 나머지 비트는 항상 0이 된다.

$$A[0,0,z] \leftarrow A[0,0,z] \oplus RC[0,0,z], \quad 0 \le i_r < 24 \quad (5)$$
$$RC[0][0][2^j - 1] = rc[j + 7i_r], \ 0 \le j \le 6$$
$$rc[t] = (x^t \bmod (x^8 + x^6 + x^5 + x^4 + 1)) \bmod x, \ 0 \le t \le 167$$

ι단계는 라운드 변수 i_r을 사용하므로 라운드 간에 차이를 만들어 대칭 특성을 파괴한다. RC[0,0,z]는 라운드 변수 i_r을 사용하여 룩업 테이블(lookup table) 혹은 조합 회로로 구현할 수 있다. ι단계는 첫 번째 레인 $L[0,0]$에만 영향을 주지만 다음 라운드의 θ와 ρ단계의 확산 기능을 통해 24 라운드의 반복 동작을 거치는 동안 ι단계의 결과가 전체 레인에 확산된다.

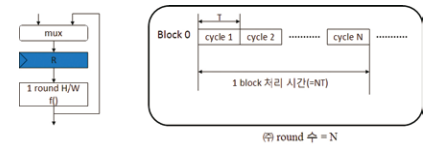
기술동향2

SHA-3의 구현 방안

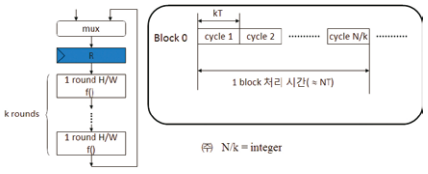
현재 SHA-3 알고리즘은 현재 다양한 구조로 ASIC 또는 FPGA로 구현되고 있다[7-9]. 응용 분야의 성능과 면적 요구 조건에 따라 크게 3가지 구조로 구현되고 있다.

- 반복 연산 구조 : 라운드 반복 함수를 구현한 후 이를 반복하여 활용하는 구조
- 파이프라인 구조 : 단계 혹은 라운드 단위의 파이프라인 구조
- 루프 펼침 구조 : 클록마다 2개 이상의 라운드를 구현하는 구조

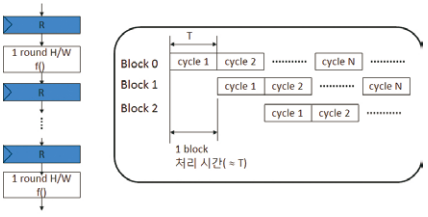
그림 8은 SHA-3에 대한 일반적인 3가지 구현 방안을 나타낸다. 단, 모든 구조에 메시지를 블록의 정수 배로 만드는 패딩 연산 블록이 별도로 필요하다.



(a) 반복 연산 구조



(b) 루프 펼침 구조



(c) 파이프라인 구조

그림 8. SHA-3에 대한 대표적인 3가지 구현 방안

향후 전망 및 맺음말

본 원고에서는 새로운 암호학적 해쉬 함수 표준인 SHA-3를 살펴보았다. 해쉬 함수는 전자 서명, 암호 프로토콜, 난수 생성기 등 다양한 보안 응용에 광범위하게 사용되고 있다. 현재 SHA-2가 아직은 일반적인 사용에 있어서 안전하다고 평가되고 있으므로 당분간은 SHA-3가 SHA-2의 대체가 아닌 보완 역할을 할 것으로 판단된다. 또한, SHA-2와 SHA-3의 구조와 연산은 근본적으로 다르기 때문에, 암호 공격에 대한 대처 효과는 배가되는 장점이 존재한다. 그러나 암호화 알고리즘에 대한 공격 및 분석 기술이 점점 발전하고 있고, 반도체 기술의 발달로 병렬 및 파이프라인, 멀티 코어를 사용한 컴퓨터 기술 향상되고 있는 점을 고려할 때, 공개 알고리즘인 SHA-3 알고리즘을 고속으로 구현하는 연구와 SHA-3보다 우수한 국내 독자 해쉬 알고리즘 개발 연구가 필요하다. 그리고 사실상 SHA-3 알고리즘이 차세대 해쉬 알고리즘의 국제 표준이므로 보안 제품의 수출 증대 및 수입 대체 효과를 위해 다양한 성능 및 면적 스펙트럼을 갖는 SoC 제품과 반도체 IP 개발 및 임베디드 시스템에 내장하는 소프트웨어 개발 연구가 필요하다고 판단된다. 마지막으로 본 원고가 SHA-3에 대한 이해를 높이는데 도움이 되길 기대한다.

Reference

1 William Stalling, *Cryptography and Network Security-Principle and Practices*, 5th edition, Prentice Hall, 2010.

2 Bart Preneel, "The state of Cryptographic Hash Functions," Proceedings, *Lectures on Data Security*, Lecture Notes in Computer Science 1561, pp. 158–182, 1999.

3 X. Wang, Y. Yin, and H. Yu, "Finding collisions in the full SHA-1," in *Advances in Cryptology, Proceedings Crypto* (Lecture Notes in Computer Science, vol. 3621), V. Shoup, Ed. New York: Springer-Verlag, 2005, pp. 1–16.

4 W. Burr, "A new hash competition," *IEEE Security Privacy*, vol. 6, no.3, pp. 60–62, May–June 2008.

5 NIST, *SHA-3 Standard : Permutation-Based Hash and Extendable-Output Functions*, FIPS PUB-202, August 2015.

6 William Stalling, "Inside SHA-3", IEEE Potentials, November/December, 2013, pp. 26-31.

7 George Provelengios, etc, "FPGA-Based Design Approaches of Keccak Hash Function", Euromicro Conference on Digital System Design, pp.648-653. 2012.

8 Alia Arshad, etc, "Compact Implementation of SHA3-512 on FPGA", Conference on Information Assurance and Cyber Security(CIACS), pp.29-33, 2014.

9 Tatsuya Honda, etc. "FPGA Implementation of New Standard Hash Function Keccak", 3rd Global Conference on Consumer Electronics, pp.275-279, 2014.

저자정보

최 병 윤 교수

소 속
동의대학교 컴퓨터공학과

연구분야 컴퓨터구조, 임베디드시스템
E-mail bychoi@deu.ac.kr
Homepage http://hyomin.deu.ac.kr/~bychoi

기획칼럼1

Silvaco사 Expert

A. 목적

Layout Editor

B. 개요

Expert는 완벽한 편집 기능, 대규모 용량 처리, 신속한 레이아웃 뷰어를 갖춘 고성능 계층형 IC 레이아웃 에디터 입니다. Expert는 넷리스트에 의한 레이아웃 및 Pcell(Parameterized cell)을 통하여 높은 수준의 설계 지원을 제공합니다.

C. Supported platform

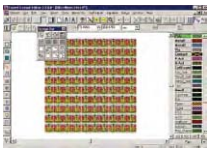
- Red Hat Enterprise (32/64bit) Linux 5, 6
- Windows XP, Windows 7 Professional (32/64bit)

D. 특징

- 통합된 DRC/LVS/LPE 및 기생 추출 기능으로, 아날로그, 믹스드 시그널, RF, 디지털 레이아웃에 생산적인 환경
- ExpertViews는 편집 기능을 제외하면, Expert와 기능면에서 동일
- GDSII 파일의 신속한 로딩, 편집 및 대규모 데이터베이스의 뷰어
- 설계 자동화에 필요한 강력한 스크립트 성능 및 C++ API를 제공
- 업계 표준 포맷을 사용하여, 물리 검증을 위해 Calibre Interactive 및 Calibre RVE와 통합
- 노드 하이라이트 기능을 제공하여, 클릭한 객체와 전기적으로 연결된 레이아웃 객체를 모두 하이라이트
- 모든 기술 레벨를 위한 사용의 편이성 – 초보자를 위한 온라인 도움말, 전문가를 위한 강력한 스크립트
- 강력한 암호화에 의해 고객 및 서드-파티의 소중한 지적 재산권을 보호 가능

생산적인 레이아웃 환경

- 10GB 이상의 데이터베이스를 몇 분(몇 시간이 아님!)만에 고속으로 로드
- 멀티-레벨 계층을 통하여 여러 윈도우에 신속하게 이동 및 확대/축소-탐색을 위한 북마크 기능 구비
- 실시간, 온라인, 배치 검증을 위해 Guardian DRC/LVS/LPE와 유연하게 통합
- CMOS, Bipolar, BiCMOS, SiGe, GaAs, InP 등에서 아날로그, RF, 디지털 회로에 생산적인 레이아웃 환경
- 명령어를 편리하게 호출하기 위해, 단축키 메뉴 및 커맨드 라인을 변경 가능



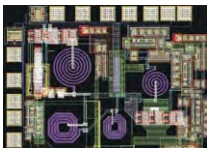
완벽하게 변경 가능한 단축키, 매크로, 툴바, 레이어, 색상, 스티플 등을 Virtuoso로부터 직접 가져와서, 레이아웃 설계자에게 익숙하고 생산적인 작업 환경을 제공합니다.

타사 디자인 플로우와 호환

- Dracula, Diva DRC/LVS/LPE 룰 덱크 지원
- RVE(Result Viewing Environment)에 필요한 Calibre 에러 리포트를 바로 읽음
- 레이어, 색상, 스티플, 단축키, 매크로, 툴바에 필요한 테크놀로지 파일을 Virtuoso에서 가져옴
- GDSII 및 CIF 데이터와 함께 기존 디자인을 가져옴

강력한 레이아웃 에디터 기능

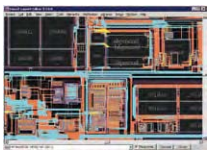
- Javascript 및 LISA 스크립트 그래픽 지원으로 Parameterized cell 생성
- 강력한 C++ API는 모든 편집 기능에 액세스
- 체크-인, 체크-아웃 라이브러리 매니저를 이용하여, 네트워크로 동일 프로젝트에 대해 동시 작업 가능
- 자동 축소/확대 및 크기 조정 기능으로 공정 이전에 드는 수고를 최소화



다용도 에디터는 아날로그, RF, 마이크로파 회로 요소에 필요한 모든 각도의 다각형을 생성하며, CMOS, Bipolar, BiCMOS, SiGe, GaAs, SiC, InP, TFT 및 기타 공정 기술의 인덕터, 파워 디바이스가 포함됩니다.

Real Time DRC

- Expert를 통해서 완벽하게 통합된 Real-Time Guardian DRC를 사용
- 레이아웃 편집 중에 대화식으로 DRC 위반을 플래그
- 레이아웃 중에 정정이 이루어지므로, 최종 DRC 검증을 대폭 단축
- Guardian DRC와 동일한 룰세트



10GB가 넘는 대용량 데이터베이스를 몇 분(몇 시간이 아님!)만에 고속으로 로드하며, 대규모 데이터베이스를 신속하게 이동 및 확대/축소할 수 있습니다. 또한, 마스크 준비 및 배선 수정에 이상적입니다.

기획칼럼2

ISSCC 2016 참가 후기 및 기술 트렌드

2016년 ISSCC(International Solid-State Circuit Conference)는 1/31~2/4일 샌프란시스코에서 개최되었다. 이번 컨퍼런스의 주제는 "SILICON SYSTEMS FOR THE INTERNET OF EVERYTHING"으로 요즘 주목받고 있는 IoT에서 반도체의 중요성을 다시 한번 강조했다고 여겨진다. Plenary 세션에서 Intel의 Bill Holt는 Moore's law를 여러 측면에서 재조명했으며, Xerox의 CTO는 IoE(Internet of Everything)를 Smart objects, Network, Automated insights라는 3개의 축으로 접근했다. NTT DOCOMO에서는 5G에 대한 기술과 미래를 내다보았고, NXP에서는 지능화 되어가는 자동차에 대한 발표를 진행하여 최근의 기술동향과 SoC의 역할에 대해 생각해볼 수 있는 시간이 되었다. 본 기고문은 ISSCC에 참석했던 전문가들이 분야별로 발표된 논문들의 주요 기술 및 차별성 등을 참가 후기의 형식으로 정리하였다.

Analog Techniques

문 용 교수 | 숭실대학교 전자정보공학부
E-mail moony@ssu.ac.kr

이 세션은 최신 아날로그 회로들의 다양성과 우수성을 보여주었으며, 특히 다양한 응용분야에서 아날로그 회로가 에너지 효율을 어떻게 개선했는지를 강조한 경우가 많았다. 본 세션에서는 연산 증폭기, Class-D 증폭기, 센서 front-end, VGA, oscillator 등 넓은 분야의 연구가 다루어졌다. 이 중 특색 있는 몇 가지 논문을 설명하고자 한다.

Class-D 증폭기는 2개의 논문이 발표되었다. 하나는 MERUS AUDIO에서 발표한 70W급 증폭기로 5-level power stage를 사용하여 전력 효율을 증가시키고 idle power는 현저히 줄이는 기술을 적용하였다. 또한, 적은 form factor 적용이 가능하도록 크기를 줄이는 연구도 진행하였다. MediaTek에서 발표한 논문은 모바일 폰에서 점점 중요해지고 있는 높은 PSRR과 선형성을 만족시키기 위해 input feed-forward 기법과 PWM Common-Mode feedback을 적용하였다. 이를 통해 118dB-PSRR과 0.00067%(-103.5dB) THD+N을 구현할 수 있었다. 아래 그림에서 파란색 부분이 출력단(V_{ON}, V_{OP})에서 CM feedback을 하는 부분이며, 입력신호는 resistor summing 방법을 통하여 "b"로 스케일링 되어 feed-forwarding 되는 것을 살펴볼 수 있다. 출력신호에서 피드백 되는 신호를 생성하는 회로를 다음 그림에 자세히 나타내었다.

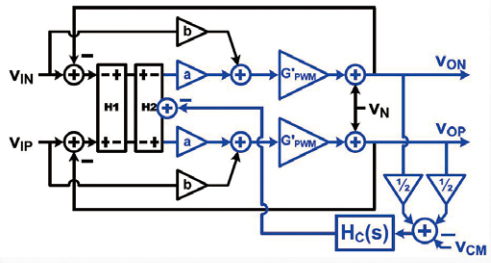


그림 1. 제안한 CDA의 시스템 구조

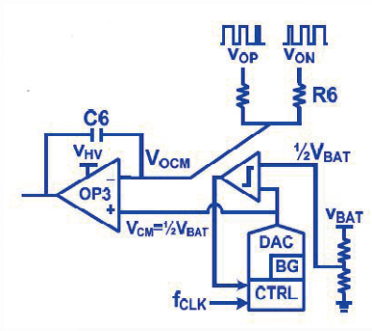


그림 2. PWM output CM control

MIT에서는 sensor front-end에 적용 가능한 chopper amplifier를 발표했으며, noise efficiency를 개선하기 위해 0.2V supply를 사용하는 입력단을 제안하였다. "Squeezed-inverter" 단으로 부르는 이 부분은 인버터를 기반으로 하며 2VDSAT으로 동작하고, 구체적인 회로는 아래 그림과 같다. 저전압 입력단 이후에는 0.8V 전원을 통해서 선형성과 swing을 확보하였다. 제안한 chopper amplifier는 biopotential 측정에 적용했으며, 74%의 효율과 0.31μW의 매우 낮은 전력소모를 보여주었다.

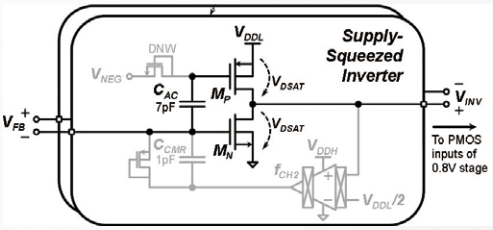


그림 3. Squeezed-inverter 입력단

Univ. of Michigan에서는 WSN(Wireless Sensor Node)에 사용되는 타이머에 switched-resistor scheme을 적용하여 ultra low power를 구현했으며, switched-capacitor를 기반으로 하는 DC-DC converter를 통해 출력 주파수의 안정성을 확보하였다. 이 논문에 적용된 switched-resistor 기반

timer의 개념은 아래 그림과 같다. 하단 부분의 캐피시터와 스위치로 구성된 switched-capacitor는 주파수를 센싱하는 부분이고 상단 부분의 저항과 스위치가 switched-resistor 부분이다. 이 외에도 thyristor-based delay cell을 사용한 VCO, 1/N replica biasing을 적용한 amplifier, 리플을 제거하는 sampler 등 다양한 접근을 시도하였다.

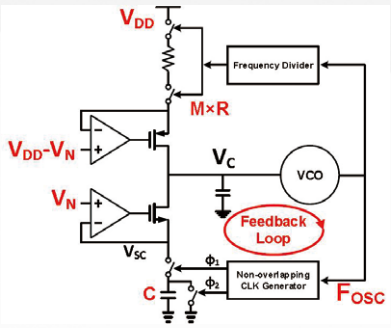


그림 4. Switched-resistor scheme을 적용한 wake-up timer 구조

마지막으로 A*STAR, DGIST, Nanyang technological university가 참여한 논문에서는 저잡음 차동 relaxation oscillator를 발표하였다. 이 논문에서는 differential swing boosting scheme을 적용하고 저잡음 및 저전력 비교기를 사용했으며, 오프셋 cancellation도 가능한 발진기를 제안하였다. 제안한 발진기의 구조는 아래 그림과 같으며, 전원 전압의 4배에 해당되는 signal swing을 얻을 수 있다. 또한 differential 비교기는 inverter를 기반으로 하고 있고, 회로는 아래 그림과 같다. 여기서 transconducatance를 최대화하고 전력 소모는 최소화하는 설계를 하였다. 이를 통해서 낮은 지터 특성과 높은 FOM의 확보가 가능했다.

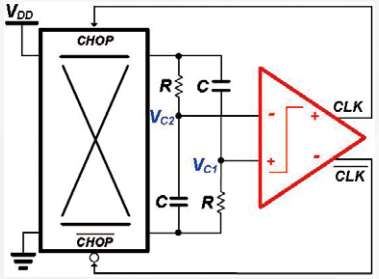


그림 5. Differential relaxation oscillator의 구조

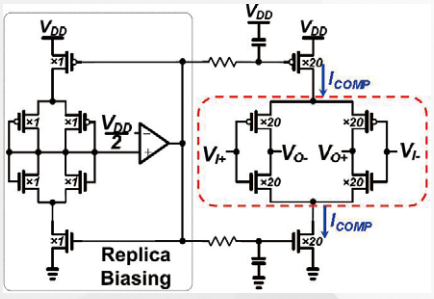


그림 6. 저전력 저잡음 차동 비교기

Low Power Digital Circuits

김 경 기 교수(저전력 고신뢰 디지털 시스템 설계, 비동기 회로 설계)
대구대학교 전자전기공학부 E-mail kkkim@daegu.ac.kr

최근 IoE/IoT와 같이 에너지가 제한된 플랫폼에서의 높은 성능에 대한 요구는 모든 CMOS 디지털 회로 블록들에 대한 지속적인 기술적 혁신을 불러오고 있으며, 이런 혁신은 더욱더 에너지를 효율적으로 줄이면서도 회로를 고성능으로 유지하고 향상된 확장성(scalability)으로 저비용의 보강된 보안(security)을 가지는 디지털 회로 블록의 설계를 가능하도록 하고 있다. ISSCC 2016의 "Low-Power Digital Circuits" 세션에서도 이런 연구경향의 논문들이 총 8편 발표되었다.

먼저 프랑스의 CEA-LETI에서 발표한 첫 번째 논문(#8-1)은 컴퓨팅 전력을 더 많이 요구하는 MIMO telecom 응용을 목표로 하는 비동기 링크 방식의 4x4x2 homogeneous scalable 3D NoC(network-on-chip)회로를 제안하고 65nm 공정기술에서 구현되었다. 본 논문에서는 멀티코어 설계를 위해 (2D NoC에 비해 확장성과 모듈별 chip-to-chip 통신이 우수한) 3D NoC 회로를 사용하였고, 3D NoC 회로에서 이슈가 되는 3D 통신 구조, 높은 밴드폭, 에너지 효율성, 결함 감내(fault tolerance) 등을 고려한 기술이 제안되었다. 제안된 회로는 top die와 bottom die의 2개의 층으로 구성되고, 각 층 내에서는 32b 비동기와 GALS 방식의 NoC를 기반으로 2x2 RX/TX MIMO 구조를 지원하며, ARM1176 Host CPU로 구성된 heterogeneous multi-core와 18개의 accelerator(DSP, Telecom IPs 등)로 구성되었다. 층 사이의 3D interconnect는 4개의 비동기 3D 수직 링크를 가지는 4x4x2(32 NoC 라우터) 3D NoC 방법을, 네트워킹의 견고성(robustness)을 위해서 3D NoC는 저전력의 4-phase 4-rail의 handshake를 가지는 QDI(Quasi Delay-Insensitive) 비동기 회로를 사용해서 설계되었다. 수율(yield)을 증가시키고 생산 테스트를 위해 TMR(triple-modular redundancy)을 사용한 JTAG와 boundary scan 방법을 이용한 test and fault tolerant architecture가 적용되었다. 그림의 3D 단면과 같이 비용을 최적화 하고자 디자인과 마스크가 top die와 bottom die 사이에서 공유되도록 하였다. 제안된 3D NoC architecture는 326Mb/s의 최고 데이터 전송 속도를 가지면서 0.32pJ/b의 낮은 전력을 보여주었다.

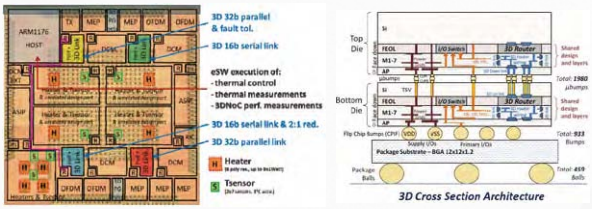


그림 1. 3D NoC architecture and cross section(#8-1)

#8-2와 #8-3 논문은 새로운 디지털 LDO(Low-Drop-Out) 레귤레이터(regulator) 회로들을 제안하고 있다. 일반적으로 하나의 칩에서 파워 영역의 많은 부분은 LDO 레귤레이터에 의해 설계되고 있지만, 부하 전류에서의 크고 빠른 변화를 보상하기 위해 사용되는 크기가 큰 off-chip 출력 커패시터(capacitor)가 기존 LDO 설계에서 주된 오버헤드(overhead)가 되고 있다. 두 논문에서는 이런 큰 off-chip 출력 커패시터를 칩 내부로 넣어 집적화하거나 사이즈를 줄이는 방법들이 제안되었다. 하지만 이런 출력 커패시터의 크기를 줄이거나 칩 내부에 집적화하기 위해서는 control loop latency가

짧아져야 하므로, 높은 샘플링 주파수를 가지는 동기방식의 time-driven digital LDO나 고속의 증폭기를 가지는 analog LDO를 사용해야 되지만 전력 소비가 문제가 되고 있다. Columbia University에서 발표한 #8-2 논문에서는 이런 전력 효율과 latency 사이의 상관관계를 없애기 위해, 즉 저전력을 유지하면서 짧은 latency를 가질 수 있도록 event-driven 방식의 디지털 LDO 레귤레이터를 제안하였다. 제안된 event-driven 디지털 LDO는 65nm 공정 기술에서 구현되었고, 측정 결과에서 제안된 LDO는 Vin=0.5V, Vout=0.45V에서 400μA를 공급하고, 10%의 VDROOP의 제한 조건에서 칩 내에 집적화된 출력 커패시터의 크기는 단지 0.4nF 이었다. 또한, 96.3%의 최고 전류효율을 가지는 것을 측정 결과에서 보여주었다. 삼성에서 발표한 다음 논문(#8-3)은 LDO가 포함된 PMIC와 모바일 AP(application processor) 사이에 존재하는 외부 커패시터 수를 줄이기 위해 PMIC에서의 LDO를 AP에 집적화하여 복잡한 파워 라우팅(power routing)을 줄이고자 하였다. 그리고, fast transient response, large capability of current, low power consumption을 동시에 이루고자 shift register를 사용한 fine loop와 current-mirror flash ADC를 사용하는 coarse loop를 사용한 새로운 디지털 LDO 레귤레이터를 제안하였다. 제안된 LDO는 28nm 공정 기술에서 0.021mm^{2}의 사이즈를 가지고 200mA까지의 부하 전류를 제공하였다. 또한, 최대한 제공될 수 있는 전류 부하의 90% 부하 변이에 대해서 약 120mv의 출력 전압 드룹(droop)을 보여주었다.

인텔에서 발표한 #8-4의 논문은 런-타임(run-time)동안 온도나 노화(aging)에 의한 변이에 의해 발생하는 회로지연 감소를 모니터링 하는 in-situ Tunable Replica Circuit(TRC)의 결과를 적응형 전압 스케일링(AVS: Adaptive Voltage Scaling) 회로에 적용, 공급 전압을 동적으로 조정하여 지연 감소를 보상할 수 있는 22nm 공정 기술에서 제작된 graphics execution core를 발표하였다. 더불어, 기존의 파워 게이팅(PG: Power Gating) 구조를 고정된 큰 저항을 가지는 top primary PG와 동적으로 크기가 결정되는 secondary PG로 나누고, 휴면 모드에서 활성화 모드로 천이할 때 TRC의 결과를 사용해서 secondary PG의 사이즈를 변경하여 wake-up 시에 발생하는 전압 드룹(droop)을 줄여서 guard band/delay margin 시간을 줄일 수 있다는 것을 보여주었다. 측정된 결과에서 AVS는 최악의 온도와 노화 조건과 0.4V(0.8V) 전압에서 33%(14%)의 에너지 감소를 각각 보여주었고, 제안된 동적 PG는 0.6V(0.8V) 전압에서 14.5%(7%)의 에너지를 감소 시키면서 11%(8%)의 평균 가상 레일(virtual rail) 전압 감소를 각각 보여주었다.

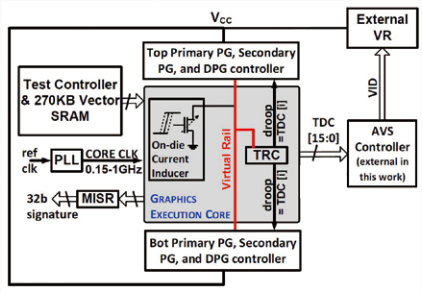


그림 2. Chip block diagram(#8-4)

다음 University of Michigan 에서 발표된 논문(#8-5)에서는 작은 IoT 시스템을 위한 완전히 칩에 집적화되는 작은 사이즈의 PMU(Power Management Unit)가 제안되었다. 제안된 PMU는 0.9V~4V의 범위에 있는 입력 전압을 3개의 고정된 전압(0.6V, 1.2V, 3.3V)으로 각각 변환하는 switched-capacitor DC-DC 변환 회로를 포함하고 있다. 제안된 회로는 1V~4V의 넓은 입력 범위에서 60% 이상의 변환 효율과 20nW~500uW의 출력 전력을 유지함을 보여주었다. Nvidia에서 발표한 #8-6 논문에서는 큰 GPU에서 큰 전력을 차지하는 global communication power을 줄이기 위해 기존의 CMOS repeater 연결을 사용하지 않고, 전압을 1/2로 줄여서 전체 global communication power를 이론적으로 1/4로 줄이고자 stacked CMOS inverter 들로 구성된 charge-recycling bus 개념을 향상시킨 balanced charge-recycling bus(BCRB) 기술을 제안하였고, 버스의 와이어(wire)들에서 신호들을 서로 반대로 흘러가게 하여 cross-talk 영향과 flip-flop의 수를 줄여 클럭에서 소모되는 전력을 줄이는 low crosstalk contraflow wiring 기술도 제안하였다. 측정 결과는 16nm FinFET 공정에서 0.6V~0.8V 전압 범위에서 버스 길이를 6~12mm 변화시켰을 때 하나의 repeater bus에서 1.7~2.6Gb/s/wire의 속도를 가지는 임의의 데이터에 대해서 6.5~23.3fJ/b/mm의 전력 소모를 보여주었다.

삼성에서 발표한 #8-7 논문에서는 각 칩 자체의 고유한 특성(size, doping concentration, mobility, and oxide thickness 등) 변이를 이용하여 유일한 암호화 키(security key) 또는 칩 ID를 발생시키는 PUF(Physically Unclonable Function) 회로를 제안하였다. 제안된 PUF는 문턱 전압(threshold voltage)의 변이를 이용한 간단하고 크기가 작은 PUF 셀을 기반으로 하며, PUF 셀은 전력과 노화의 영향을 줄이기 위해 파워 게이팅을 구조를 사용하여 회로 부팅시간 동안에만 PUF 셀을 작동시켜 암호화 키를 발생시킨다. Thermal noise, voltage/temperature 변이, 노화 현상 같은 자연적으로 발생하는 노이즈에 의한 에러율을 줄이기 위해 안정화되지 않은 PUF 셀을 막는 방법(valid-map)을 사용하여 BER(Bit Error Rate)를 75%까지 향상시켰고, majority voting를 사용하여 BER을 0.00713에서 3.59E-6R 향상시켰고, 마지막으로 BCH ECC(Error Correction Code)가 적용되어 2.01E-38까지 향상시켰다. 스마트카드 칩을 위해 사용될 전체 PUF 회로는 45nm 공정에서 제작되었고, 크기는 3.78x1.4um^{2}이다.

마지막으로 University of Michigan에서 발표한 #8-8 논문은 앞서 기존에 발표된 EDAC(Error Detection and Correction)의 방법과는 다르게 flip-flop에서 발생하는 전류를 측정하여 PVT 변이나 노화 효과로 인해서 발생하는 동기 회로에서의 데이터 에러를 발견하게 되고, 에러가 발생되면 clock gating 방법을 사용해서 에러가 발생되지 않도록 클럭 주기를 늘려주는 방법(iRazor)을 사용하고 있다. 제안된 iRazor에서 사용되는 current-based detector는 단지 flip-flop에 3개의 트랜지스터를 추가한 것으로 4.3% 정도의 사이즈 오버헤드를 가지고 있다. 본 논문에서 iRazor는 ARM Cortex-R4에 적용되었고, 40nm 공정 기술에서 제작되었다. Typical corner에서 제작된 칩은 1.3배의 throughput gain이 발생되었고, 13.6%의 사이즈 오버헤드에 45%의 에너지 감소를 가져왔다.

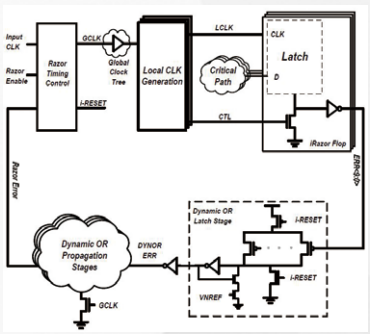


그림 3. Diagram of overall structure of EDAC technique(#8-8)

Clock Generation

조 성 환 교수(Clock generation and CMOS Sensors)
KAIST 전기 및 전자공학부 **E-mail** chosta@kaist.ac.kr

예년처럼 올해도 Clock generation 회로는 ISSCC의 여러 분과에서 다루어졌다. RF 및 wireless 분과에서는 무선 시스템을 위한 low-phase noise, low-spur frequency synthesizer를 다루었고(Session #2, #9), wireline 분과에서는 high-speed link에 응용될 수 있는 low-jitter PLL, DLL technique을 다루었다(Session #10). DSP, processor에 응용되는 Digital PLL은 올해 새로 생긴 Digital Circuits Subcommittee에서 다루어졌다(Session #19). 이 네 세션에서 발표된 PLL, DLL과 이와 관련된 회로들(VCO, TDC)을 합치면 총 23편인데, 이 중 몇 가지 주목할 만한 논문을 살펴본다.

#2.3은 구조적으로 좀 색다른 논문이다. Integer-N PLL을 먼저 만든 후 이의 noise를 filter할 수 있는 DLL을 추가로 달았는데, 보기에는 그럴 듯 해 보이나, 첫 단의 Integer-N PLL을 너무 좋지 않게 설계했으며, 오히려 Injection locking 또는 MDLL의 기법을 Integer-N PLL에 사용했다면 이러한 기법을 굳이 쓰지 않아도 될 것으로 보인다. Reference spur가 큰 것이 약점이며(-45dBc), Multiplication ratio가 그리 큰 것도 아니고(31), FoM 성능은 -234 정도로 우수한 편이지만, 기존 논문들과 큰 차이를 보이지는 않는다. #2.5에서는 성능이 매우 좋은 VCO를 선보인다. Transformer를 사용했는데, 기존 구조와는 다르게 PMOS-NMOS complementary 구조를 구현하여 common-mode resonance를 이용할 수 있도록 했다. 성능이 어마어마하게 좋은데, 특히 1/f noise corner를 28nm 공정에서 200kHz 정도로 낮추고 게다가 FOM을 -195dB정도까지 가져간 것은 매우 고무적이다. 기존에 좋은 성능을 보였던 Class-C type의 VCO가 bias generation에서 설계의 어려움이 있었다면 이번 구조는 이에 비해 훨씬 더 간단하여, 앞으로 많은 사람들이 활용할 수 있을 것으로 기대된다. Chip photo를 보면 transformer의 layout이 특이한데, 혹시 이것이 성능을 향상시키는 핵심은 아닌지 좀 더 살펴봐야 한다.

#2.7에서도 1/f noise가 매우 낮고 FOM이 좋은 ring oscillator를 선보이는데, frequency가 낮은 ring oscillator를 여러 개 만들어 oscillator의 impulse sensitivity function을 낮춘 이후 phase를 적절히 섞어서 구현하였다. 성능이 전체적으로 좋으나 한 가지 문제는 phase를 섞으면서 spur가 꽤 크게 보인다는 것이다. #2.8에서는 injection locking 회로에서 문제가 되었던 locking range를 oscillation amplitude를 통해 파악하고 이를 보정하는 회로가 소개되었고, 다른 injection locking 회로에도 사용될 수 있을 것으로 기대된다.

#9.6에서는 기존의 sub-sampling PD에서 이용된 높은 전압변화(high dv/dt slope)를 fractional-N PLL의 linear TDC에 활용했고, 이를 통해 state-of-the-art 성능을 달성하였다. 최근들어 Digital PLL의 성능을 높이기 위해 time-domain signal 정보가 아닌 analog voltage를 활용하는 논문들이 보이는데, 이 논문도 같은 맥락에서 볼 수 있다. (#19.7도 voltage 정보를 활용)

#10.5에서는 Spur cancellation이 되는 fractional-N PLL을 선보인다. 결국은 FIR filter의 null에 해당하는 spur을 없애는 것이고 이 null을 정확히 찾아갈 수 있도록 adaptive filter를 추가하였다. -73dBc 이하의 성능이 매우 훌륭하다. #10.7에서는 Ring-VCO에서 Injection locking를 할 때 spur을 줄이기 위해서 oscillator 전체의 replica를 사용하는 것이 아니라 delay cell 하나만의 replica를 사용한 참신한 구조이다. 성능이 매우 우수하며 supply와 temperature 변화에서도 제시한 회로가 강인하다는 것을 실험을 통해 보여준 매우 완성도 있는 논문이다.

Digital PLL에서는 reference의 rising 및 falling edge를 모두 사용하여 MDLL의 spur를 줄인 논문(#19.3)이 주목할 만 하고, supply noise를 줄이는 논문이 두 편 있는데 이 중 supply cancellation 회로의 보정을 background로 하는 #19.5의 구조가 흥미롭다. 그러나, power supply noise의 크기가 바뀔 때 동작을 어떻게 할지 의구심이 생기는 회로이다. #19.8은 Time-domain signal만을 활용하여 loop filter를 꾸몄는데 이로 인해 voltage domain에서 필요한 capacitor가 필요 없게 된다. 결과적으로 면적이 기존 PLL에 비해 10배 이하인 PLL이 구현되었다.

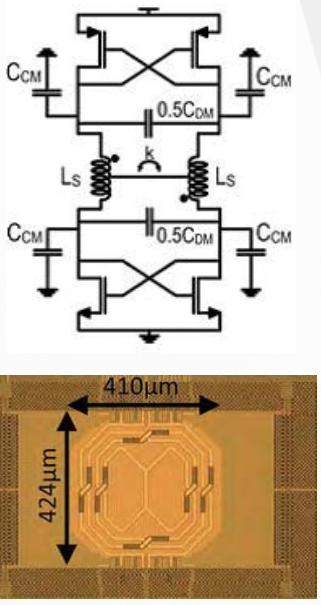


그림 1. #2.5의 Low-noise를 갖는 complementary VCO

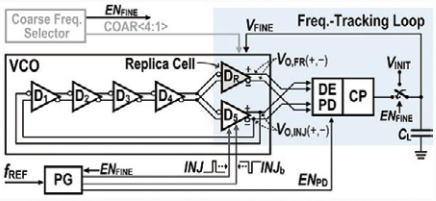


그림 2. #10.7의 Injection-locked clock multiplier 구조

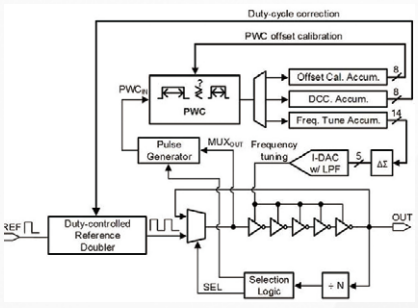


그림 3. #19.3의 Double injection MDLL 구조

Data Converter

류승탁 교수 | KAIST 전기 및 전자공학부
E-mail stryu@kaist.ac.kr

2016년 ISSCC Data Converter 분과에서는 두 개의 세션에서 총 16편의 논문이 발표되었다. 예년과 달리 올해에는 상당히 많은 oversampling data converter 논문이 제출되었고, 발표된 논문의 절반을 차지하였다. 또한, 두 개 이상의 ADC 구조를 결합한 hybrid 구조들이 많이 시도된 점이 눈에 띄었다. U.T. Dallas에서는 Continuous-Time(CT) Delta-Sigma Modulator(DSM)의 quantizer로 SAR ADC를 적용하여(SAR-Assisted CT DSM) SAR ADC의 동작 후, DAC에 남게되는 quantization error를 딜레이를 거쳐 loop filter로 injection 함으로써 Noise Coupling(NC) 기능을 용이하게 구현하였다(#15.1). NC 과정에 CT RC network을 추가로 거치게 하여 2nd order noise shaping이 가능토록 하여, 4차 loop filter를 이용하면서도 6차 DSM의 성능을 얻었다. 이러한 효과적인 구조 덕분에 1GHz 미만의 sampling 주파수와 x10의 낮은 OSR로도 45MHz의 넓은 신호 대역을 달성하였고, 비슷한 사양들 중에서 가장 우수한 168dB의 Figure-of-Merit(FoM)를 얻었다.

인도의 IIT Madras에서는 고해상도 DSM에서 flicker noise를 줄이기 위해 흔히 사용되는 chopping 기법에 의한 shaped quantization noise aliasing 문제를 해결하기 위해 FIR DAC을 이용하는 방법을 소개했다(#15.4). 기존에 DSM에 사용되던 FIR DAC은 1b feedback DAC에 의해 첫 단 opamp의 summing node가 크게 흔들려서 발생하는 nonlinearity의 문제를 줄이기 위한 목적으로 주로 사용되었으나, FIR DAC이 매 fs/(# of taps)의 주파수마다 null이 생긴다는 점을 이용하여, chopping에 의한 tone들이 alias되는 주파수에 이 null이 생기도록 FIR tap 수와 chopping 주파수를 선정했으며, 이를 통해 매우 낮은 flicker 특성을 달성하여 경쟁력 있는 FoM을 보였다.

네덜란드의 Delft University of Technology에서도 오디오 대역의 ADC를 발표했는데(#15.7), 기존 DC 신호처리에 국한되던 zoom-ADC 구조를 이용하되, coarse ADC로 사용되는 SAR ADC가 conversion을 마칠 때마다 fine ADC로 사용되는 DSM의 reference를 그에 맞추어 변경해주고, 빠른 신호에 대응하기 위해 두 stage간의 redundancy 범위를 기존대비 넓힘으로써 30kHz 신호대역까지 처리할 수 있도록 설계하였다. Inverter-based integrator 구현을 통해 0.16um 공정에서 178dB 수준의 높은 FoM을 달성하였다.

Analog Devices에서는(#15.5) 휴대통신의 발전에 따라 수백 MHz 이상으로 요구되는 RF bandwidth에 대응하고 image rejection filter의 부담을 덜어주기 위한 목적으로 465MHz라는 매우 넓은 대역폭을 갖는 1-2 MASH 구조의 CT DSM을 28nm CMOS 공정을 이용하여 구현하였다. 이제까지 발표된 CMOS DSM으로는 가장 높은 8GHz의 클럭주파수를 사용하였고, 930mW의 전력을 소모하면서 65dB 수준의 최대 SNDR을 달성하였다.

대만의 MediaTek에서는 고해상도 센서 응용을 위해서 noise shaping 기능을 갖는 SAR ADC를 구현했는데(#27.2), 기존의 noise-shaping SAR ADC와 차별화되는 큰 특징은 DAC의 mismatch 에러가 1차 shaping 되는 기법을 제안하여 SFDR 105dB에 달하는 매우 높은 선형성을 달성했다는 것이다. SAR ADC가 새로운 입력을 샘플할 때 이전 DAC의 LSB code를 SAR ADC에 그대로 연결해줌으로써 이전 샘플의 conversion에 포함 되었던 LSB단의 mismatch 정보가 새로운 입력을 conversion할 때 자동적으로 상쇄되도록 하였다(그림 1). MSB 부분의 mismatch는 data weighted averaging(DWA)을 통하여 개선하였다.

MediaTek에서 발표한 또 다른 논문은 고해상도 SAR ADC에서 노이즈 조건을 만족시키기 위해 비교기가 많은 전력을 소모하는 점을 개선하기 위해서 MSB는 7b SAR ADC로 얻고, LSB는 low- noise 6b digital single-slope ADC를 결합한 12b 100MS/s ADC를 보였다(#27.4, 그림 2). 기존에 발표되었던 digital single-slope ADC에서의 delay line에 interpolation 기법을 적용하여 CDAC의 부담을 줄였고, 28nm CMOS 공정을 이용하여 2.63fJ/c-s의 Walden FoM을 달성하였다.

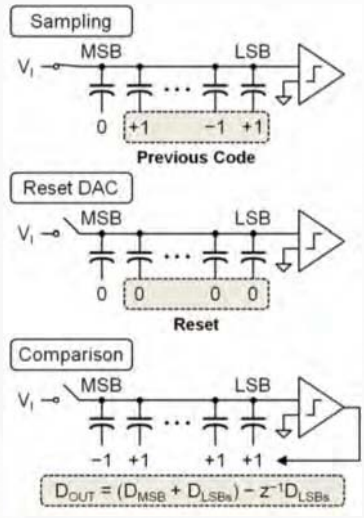


그림 1. DAC mismatch error shaping(#27.2)

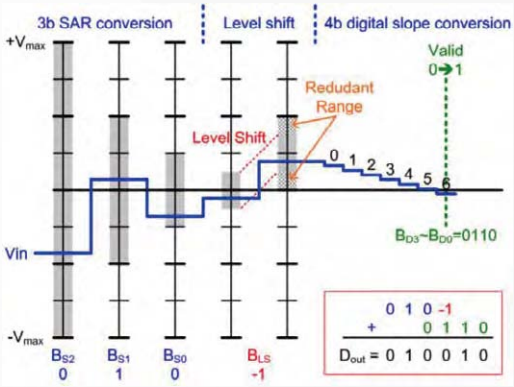


그림 2. SAR+Single-slope hybrid ADC(#27.4)

마지막으로, Broadcom에서는 16nm CMOS 공정을 이용하여 CMOS 13b ADC로는 가장 빠른 SHA-free 4GS/s ADC를 발표했는데(#27.6), 현재 고속 ADC 구현을 위한 일반적인 설계 방법인 다수의 SAR ADC를 이용하는 time-interleaving 구조는 채널간의 부정합으로 인해 높은 선형성을 얻기가 어렵다는 이유로 파이프라인 구조를 선택했다. Capacitor sampling network만 4채널로 interleaving 하였을 뿐, MDAC을 위한 amp는 stage 당 하나씩만 두어 sampling capacitor들이 share하게 함으로써 노이즈와 distortion을 줄이는 노력을 하였다. Share된 opamp에서 발생하는 memory

effect와 inter-stage coupling effect는 multi-stage concurrent MDAC equalizer(FIR equalizer)를 두어 background로 calibration할 수 있도록 했다. 4개의 sampling network 간의 skew를 줄이기 위해 single master clock을 이용하여 4 phase의 sampling clock을 re-synchronize 하였다. 100fs 이하의 낮은 지터 구현을 위해 clock generator를 위한 별도의 internally regulated supply를 공급하고, sharp한 clock을 생성하도록 하여 clock generator가 ADC 전체 전력소모의 25%를 차지하였다. 그 결과, 1.5GHz 입력에서 56dB의 SNDR을 얻었고 300mW의 전력을 소모하였다.

이상, 2016년 ISSCC에서 발표된 몇 가지 흥미로운 설계들에 대해서 소개했는데, 발표된 ADC들의 전반적 성능 추이는 IEEE Solid-state Circuits Magazine Winter 2016호의 ISSCC trends에 잘 정리되어 있으므로 이를 참고하기를 권한다.

RF Frequency Synthesis Techniques

신 현 철 교수(RF/아날로그 회로, RF 주파수합성기)
광운대학교 전자융합공학과 **E-mail** hshin@kw.ac.kr

RF 주파수를 합성하고 발생시키는 회로는 통신, 센싱, 이미징 등 여러 분야에서 필수적인 요소 블락이다. 본 세션에서는 수GHz에서 최대 0.56THz까지의 주파수 발생/합성 회로 관련 논문이 총 9편 발표되었다.

2.1 논문은 CMOS 회로로서 지금까지 발표된 연구 중 최고의 주파수인 560GHz 주파수 합성기를 개발한 내용이다. 0.5-0.6 THz는 우주 관측 등에 사용되는 주파수 대역이다. VCO는 Triple-Push VCO로서 3차 고조파를 효율적으로 발생시키는 구조를 사용했고, 바로 이어서 두개의 ILFD를 적용하여 고주파 동작이 가능하도록 하였다. 2.2 논문은 5G mmWave에서 MIMO 구조에 응용이 가능한 28GHz Coupled-PLL을 구현한 결과이다. 다수의 PLL이 필요한 시스템에서 PLL을 cascade 구조로 구현하는 것 보다는 coupled 구조를 적용함으로써 전체 출력 신호의 성능이 향상됨을 실험적으로 증명하였다. 2.3 논문은 최근 많은 주목을 받는 Ring-VCO 기반 PLL에 관한 것이다. Ring-VCO 기반 PLL은 기존 LC-VCO를 사용하는 것에 비해 전류소모를 낮출 수 있고 대역폭을 높일 수 있는 것이 장점이지만, Ring-VCO의 높은 위상잡음이 기술적 한계이다. 이를 해결하기 위해 Ring-VCO 기반 위상잡음이 높은 Type-II PLL을 DLL에 통과시켜 성능을 향상시키는 기법을 제시하고 구현하였다. 2.4 논문은 2-16GHz VCO 포함 Fractional-N PLL에 관한 것이다. SiGe BiCMOS 공정을 이용하였다. 본 논문은 산업체 논문으로서 새로운 회로 설계 기법 보다는 2-16GHz의 광대역에서 우수한 성능을 구현한 내용에 초점을 맞추고 있다. 2.5논문은 5GHz CMOS LC VCO에서 flicker corner를 200kHz로 구현한 것으로서 0.5mW의 낮은 전력 소모와 195dBc/Hz의 우수한 FoM을 얻음으로써 IoT 응용에 적합함을 주장하고 있다. 논문의 핵심은 Flicker Corner를 낮추기 위해 Common-Mode Resonance를 적절히 tuning하는 회로를 삽입한 것이다. 2.6논문은 BiCMOS 공정을 이용하여 190GHz VCO를 구현했고 최대 출력전력을 -2.1dBm 얻은 것이다. 특히, 20.7%의 넓은 Tuning Range를 얻기 위해 두 개의 VCO를 Even/Odd-mode로 스위칭하는 기법을 적용하였다. 2.7 논문은 1.7-3.5GHz 35-stage Ring-VCO를 구현하였다. Flicker Corner 주파수를 90-150kHz로 낮추기 위해서 Time-interleaving 구조를 제시하고 실험적으로 증명하였다. 2.8 논문은 26-29GHz Injection-Locked Oscillator에서 기준이 되는 입력주파수에 따라 자동으로 적절한 주파수 대역을 설정하는 Frequency-Locked Loop 회로에 관한 것이다. 기본적으로 ILO가 제대로 lock을 하지 않을 때, 출력의 진폭이 변하는 현상을 이용하여 FLL을 구현하였다. 2.9논문은 Digital-to-Time Converter로서 2GHz에서 244fs resolution과 1.2ps peak-INL을 갖는 회로에 관한 것이다.

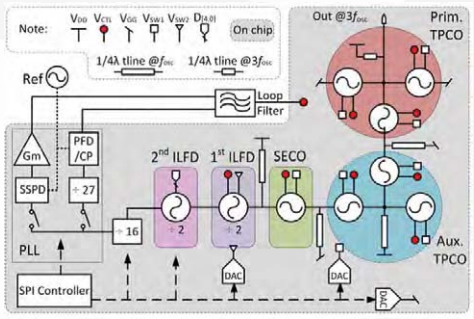


그림 1. 0.56THz 주파수 합성기 구조(2.1논문)

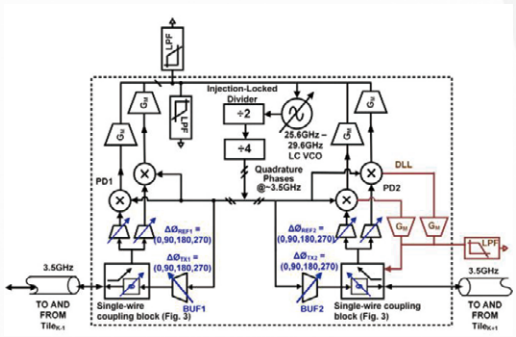


그림 2. Coupled-PLL에서 단위 PLL구조(2.2 논문)

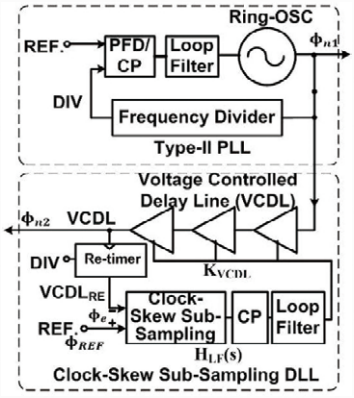


그림 3. 2.1GHz Cascaded PLL 구조(2.3 논문)

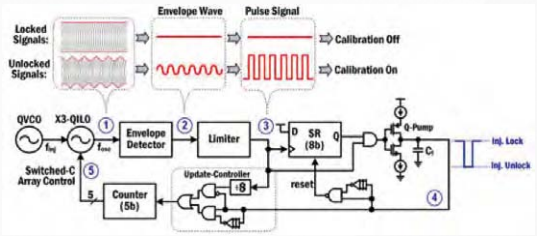


그림 4. ILO의 FLL 동작 원리(2.8 논문)

mm/THz-wave ICs

송호진 교수(초고주파 회로 및 시스템)
POSTECH 전자전기공학과 E-mail hojin@postech.ac.kr

최근 차세대 이동통신 기술인 5G 무선 시스템이 주목 받고 있는 와중에 개최된 이번 ISSCC 2016에서 약 30GHz 이상의 mm/THz-wave 회로들 세션 #3, #20, #25에서 약 14편이 발표되었다. 하지만, 정작 5G에 관한 논문은 두어 편에 불과하였다. 이는 아직 5G 시스템에 대한 개념정의나 시스템 구조에 대한 논의가 완전히 끝나지 않은 상황을 반영하는 것으로 생각된다. 오히려 100GHz 이상의 대역에서 동작하는 THz 관련 논문이 7편 이상 발표되었다. 특히 THz의 대표적인 응용분야라 할 수 있는 이미징 시스템과 관련되어 별도의 세션이 개설된 점이 특히 주목할 부분이다.

먼저 100GHz 이상의 대역에서 살펴보면, 히로시마 대학 연구팀은 300GHz 대역에서 최대 100Gbps 이상의 무선 데이터 전송이 가능한 송신기를 소개하였다. 40nm Bulk CMOS 공정을 이용한 이 결과는 회로 내에서 신호의 손실을 최소화하고 최대 출력신호를 확보하기 위해 16개의 Cubic mixer를 4개의 quad-rat-race coupler를 이용하여 병렬 배치하였다. 그 결과 275-305GHz 대역에서 17.5Gbps 32-QAM 신호를 최대 6개의 채널을 통해 전송이 가능하였다. 최대출력이 약 -14.5dBm으로 실제 시스템을 위해서는 많이 부족하고 기본적으로 대역폭이 좁아질 수 있는 구조를 사용한 한계는 있지만, 최대 100 Gbps 이상의 무선 데이터 전송이 가능한 송신기를 CMOS를 이용하여 구현했다는 점은 평가할 부분이다. #20.4에서는 300GHz 고효율 CMOS 신호 발생기를 선보였다. 신호의 출력 파워가 늘 부족한 THz 대역에서는 높은 출력신호를 얻기 위해 On-chip 안테나와 집적된 다수의 발진기를 사용하여 free-space power combining을 하는 구조는 이전에도 많이 선보인 적이 있다. 이런 구조에서는 발진기 사이의 phase lock이 중요한데, 주파수가 높은 만큼 칩 내에서조차 동기화가 상당히 어려워진다. 하지만 Tel Aviv Univ. 그룹에서는 loop 안테나를 이용함으로써, 이웃한 발진기 사이에 magnetic coupling을 유도하고, phase lock이 무선으로 이루어지게 하였다. 이는 앞으로 대형 array를 통해 THz 대역 고출력 신호원 구현에 중요한 기술로 판단된다. #25.2에서는 THz 의 중요한 응용 중 하나인 spectroscopy용 heterodyne receiver IC가 소개되었다. 이 논문에서 특히 관심을 끄는 것은, grounded coplanar waveguide와 coplanar strip lines 각각의 dominant mode가 서로 orthogonal하다는 점을 믹서 회로에 적용하여 RF, LO, IF간 isolation을 개선함과 동시에 매우 컴팩트한 레이아웃으로 전송 선로에 의한 THz 신호의 손실도 최소화 하였다. 그 결과 250 GHz 중심 주파수에서 40%에 가까운 광대역 특성을 얻을 수 있었다. #25.3의 THz spectroscopy용 IC또한 그 아이디어가 매우 돋보이는 논문이다. 일반적으로 CW THz spectroscopy 시스템은 heterodyne 혹은 homodyne 구조의 수신기가 주로 사용되어 왔다. 하지만, 이번 Princeton 대학팀은 광대역 수신 on-chip 안테나 내 전류 분포가 주파수마다 다른 점에 착안, 안테나면 내에 다수의 detector를 집적하여 전류분포를 측정할 수 있는 구조의 수신기를 만들었다. 이렇게 이미지화된 전류분포는 특정 주파수에 따른 기준 전류분포의 데이터베이스와 비교하여 최종 spectroscopy 신호를 얻을 수 있다. 결국 receiver IC는 발진기나 믹서가 전혀 필요없는 새로운 구조에서 40-300GHz의 광대역 분석이 가능하게 되었다. 100GHz 이하 CMOS를 이용한 mm-wave 대역 회로는 지난 수년간 활발한 연구가 진행되어왔다. 특히 60GHz 무선 및 70-GHz 대역 레이더용 IC가 집중적으로 논의 되어왔다. 하지만, mm-wave front-end IC의 상당수는 output power, noise figure, DC-to-RF efficiency 등의 특성에서 낮은 주파수 대역에서 동작하는 IC들의 특성에 비해 한참 뒤지는 결과를 보여주고 있다. 이는 CMOS 소자의 기본 특성뿐 아니라 소자 모델의 신뢰성, 높은 conductive/dielectric loss 등의 문제가 복합적으로 관련되어 있다. 이러한 점들은 앞으로 mm-wave 대역 5G 시스템의 상용화를 위해 집중적으로 논의가 예상되는 이슈들이다. 이와 관련해서 논문 #20.6에서 Texas A&M Univ.과 Qualcomm은 28-nm bulk CMOS를 다양한 크기와 bias조건에서 source/load pull 측정을 이용한 대신호 모델을 구축하고, 이를 이용해 최적의 PAE를 갖는 28-GHz 5G시스템용 전력 증폭기를 소개하였다. 신뢰성 높은 모델은 시뮬레이션을 통해서 system target spec(-25dBc EVM for 64-QAM OFDM with PAPR of 9.6 dB)의 만족 유무를 충분히 검증하고 대역폭 등 다양한 요구 스펙을 최적화한 결과를 선보였다. #20.10에서는 공진형 트랜스포머를 이용하여 28-nm CMOS 공정기방의 광대역 LNA를 소개하였다. 공진형 트랜스포머를 다단 증폭기의 inter-stage matching network으로 이용하는 것은 이제 특이한 방법이 아니다. 이번 논문에서는 이용한 3단 증폭기 사이에 사용된 트랜스포머의 Q나 mutual inductance K의 절대값뿐 아니라 sign이 대역 내 gain의 flatness에 큰 영향을 줄 수 있다는 점이 강조되었다. 이런 방법을 통해 0.8THz 이상의 gain-bandwidth product와 2dB 이내의 in-band gain flatness의 뛰어난 결과를 보여주었다.

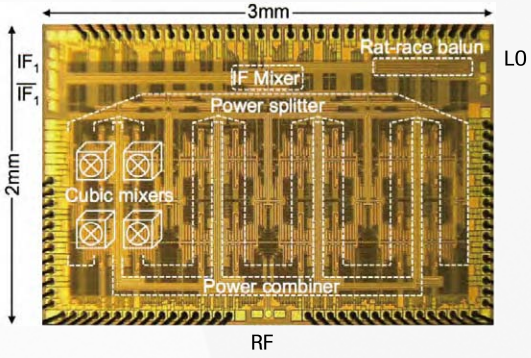


그림 1. 300GHz 32-QAM transmitter 칩사진(#20.1)

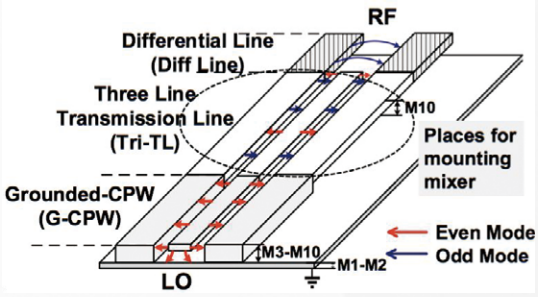


그림 2. tri-line구조를 이용한 RF/LO/IF feeding line 구조(#25.2)

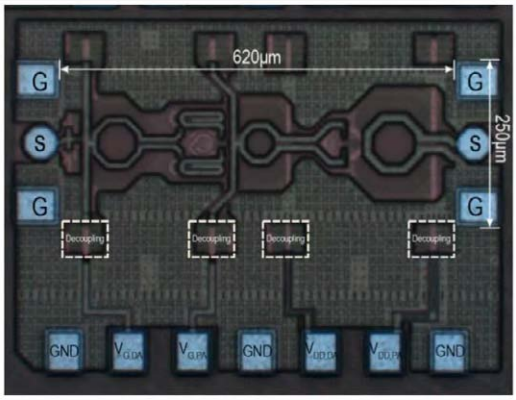


그림 3. 28-GHz 5G 시스템용 전력 증폭기(#20.6)

Advanced wireline transceivers and PLLs

최 재 혁 교수 | UNIST 전기전자컴퓨터공학부
E-mail jaehyouk@unist.ac.kr

올해 ISSCC의 Session 10에서는 "Advanced wireline transceivers and PLLs"라는 제목 아래 8편의 논문이 발표되었다. 논문은 주제별로 3편의 high-speed wireline transceiver 회로, 4편의 clock generation 회로, 1편의 clock and data recovery(CDR) 회로로 나눌 수 있다. 발표 기관 별로는 4편의 논문이 industry에서 4편의 논문이 academia에서 발표되어 균형을 이뤘다. 지역 별로는 미국 지역 내 기관이 가장 많은 5편의 논문을 발표하였고, 아시아가 2편, 유럽이 1편의 논문을 발표하였다.

#10.1와 #10.2에서는 CPU/메모리 인터페이스 채널의 noise와 reflection에 대한 resiliency를 향상시킬 수 있는 유선통신 transceiver 회로들이 소개되었다. #10.1의 논문은 새로운 코딩 기법에 기반한 transmitter와 receiver를 설계하여, 제한된 전력 소모량으로도 고집적 메모리와의 interfacing 시에 통신대역폭(bandwidth)을 확장시키는 아이디어를 발표하였다. 미국 UCLA, 대만 NCTU, TSMC사가 함께 발표한 #10.2의 transceiver는 1개의 lane이 3개의 주파수 밴드에서 동시에 신호를 변복조(기저대역: 4-PAM, 3G/6G 대역: 16QAM)하고 송수신하는 방법으로 실리콘 면적을 줄이고 에너지 효율을 증가시켰다. 총 4개의 channel lane을 이용하여 38mW의 전력 소모로 40Gb/s의 전송 속도를 획득하였다. #10.3은 clamping 회로와 analog filte를 이용하여 차량용 이더넷의 EMC 문제를 효과적으로 해결할 수 있는 analog front-end 회로를 제안하였다.

#10.4~#10.8에서는 wireline transceiver에 범용적으로 사용될 수 있는 클락 생성 기법에 대한 새로운 연구들이 소개되었다. 이중 #10.4, #10.6, #10.7는 injection-locking 기술을 기반으로 하였으며, 세 논문 모두 PVT의 변화에 대한 injection-locking oscillator(ILO)의 자유공진 주파수의 실시간적 변화를 어떻게 효과적으로 교정할 것인지, 또한 이를 통해 PVT 변화에 따른 지터 성능의 열화를 얼마나 줄일 수 있을 것인지에 대한 연구를 주제로 하였다.

일본 Sony사는 #10.4 논문을 통하여, 기존의 reference-less ILO 기반 CDR 구조에서 사용되던 master ILO를 제거하고, 대신 ILO의 자유공진 주파수를 실시간 교정하는 주파수 교정루프를 포함한 reference-less CDR 구조를 제안하였다. Bang-bang PD 기반 주파수 교정루프의 도입으로 ILO 구조의 본래 장점인 빠른 locking 속도를 유지하면서도 동시에 넓은 capture range를 획득할 수 있다는 점이 장점이다. 한국의 UNIST는 #10.7의 논문을 통하여, ILO의 replica-cell 한 개만을 사용하여 자유공진 주파수를 실시간으로 교정할 수 있는 주파수 교정루프를 포함한 새로운 구조의 ILO 기반 주파수 체배기를 제안하였다. 본 논문에서 발표된 주파수 교정루프 구조는 기존에 발표된 ILO의 replica-VCO 등을 이용하는 dual-loop 구조들과 비교하여, 자유공진 주파수 정보 획득을 위하여 한 개의 delay-cell만을 필요로 하기 때문에 delay-cell간의 mismatch에서 발생하는 교정오차를 줄일 수 있다는 장점을 갖는다. 또한 주파수 교정루프로 인하여 VCO의 노이즈를 추가적으로 줄일 수 있는 효과도 획득하였다. 매년 꾸준히 wireline session에서 논문을 발표하고 있는 UIUC의 P. K.Hanumolu 교수 그룹은 올해도 #10.6에서 기존 ILO 기반 주파수 체배기의 한계를 극복하고 아웃풋 주파수가 fractional resolution을 획득할 수 있는 DSM 기반 ILO 구조를 발표하였다. ILO의 자유공진 주파수 교정을 위해서는 작년(2015년) ISSCC를 통하여 동 기관이 integer-N type ILO구조에 적용하여 발표하였던 pulse-gating 기법을 똑같이 적용하였으며, 여기에 delay-controlled delay-line(DCDL)을 이용하여 ILO에 인가되는 reference pulse의 injection 타이밍이 DSM의 평균값에 동기가 되도록 조정하여 fractional spur를 효과적으로 낮추었다.

USC에서 발표한 #10.5의 논문은 fractional spur들의 레벨을 낮추기 위한 feed-forward multi-tone spur cancellation 기법을 소개하였다. TDC의 아웃풋 신호들을 time domain에서 볼 때 fractional spur 성분들이 반복되는 주기가 reference 주기의 배수라는 점에 착안하여, 이들이 반복되는 주기를 찾아낸 뒤에 이들의 평균값을 이용하여 TDC 아웃풋을 교정함으로써, 매우 낮은 spur 레벨을 얻을 수 있었다. IBM research는 #10.8 논문을 통하여, 기존의 LC-VCO 기반 PLL 들이 일반적으로 적용하고 있는 coarse tuning 용 capacitor back들과 fine tuning 용 varactor들의 구분적 사용(banding strategy)에서 파생하는 문제점을 지적하였다. 본 논문에서는 dual LC-DCO/VCO를 제안했는데, capacitor bank와 varactor를 연동하여 제어하는 decoder를 도입하여, VCO의 전체 tuning range 안에서 주파수의 변화가 끊김 없이 이어지게 했고 VCO gain 또한 균일하게 유지될 수 있도록 하였다. 아이디어의 검증을 위하여 chirp 신호를 생성하는 PLL을 구현했으며, 총 8GHz가 넘는(FTR>36%) 전체 주파수 범위를 band switching 없이 연속적으로 커버할 수 있음을 보여주었다.

특집기사

상상이 현실로! ‘입는 컴퓨터’를 직접 제작한다

제12회 웨어러블 컴퓨터 경진대회

웨어러블 컴퓨터는 스마트 기기를 사용자의 신체나 의복 등에 착용 및 내장함으로써 언제 어디서나 자유롭게 이용할 수 있도록 고안된 제품을 뜻한다. 최근 스마트폰과의 연동을 바탕으로 다양한 인터넷 기반 서비스를 구현하는 제품들이 주목을 받고 있다.

KAIST 시스템설계융용연구센터에서는 2005년부터 매년 ‘웨어러블 컴퓨터 경진대회’를 개최하여 올해로 12회를 맞았다. KAIST 전기 및 전자공학과 유회준 교수의 제안으로 미래 IT 인력들에게 입는 컴퓨터에 대한 제작의 기회를 주어 한국에 반도체 고급 인력을 양성하고자 하는 목적으로 시작되어 이제는 입는 컴퓨터 기술을 선도하는 최고의 대회로 성장하였다.

IT와 패션을 결합해 ‘입는 컴퓨터’를 제작하는 웨어러블 컴퓨터 경진대회는 매년 3월부터 약 두 달 가량 홈페이지에서 접수를 받아 서류심사와 발표심사를 거쳐 본선에 진출한 10개 팀에게 시작품 제작비 100만원을 지급한다. 참가팀은 7월부터 10월 말까지 본인이 제안한 입는 컴퓨터 아이디어를 직접 제작해볼 기회를 가진다. 본선대회는 11월 개최되며, 참가팀은 자신의 작품을 심사위원 앞에서 직접 시연해보는 발표와 컨셉을 알려주는 무대공연, 전시를 체험한다. 최고의 작품을 만든 팀은 ‘미래창조과학부장관상’과 함께 ‘500만원’의 상금이 수여된다.

대회를 주관하고있는 KAIST 시스템설계융용연구센터에서는 시작품 제작비 100만원 지급뿐만 아니라 제작기간 동안 웨어러블 컴퓨터 플랫폼 및 인간–컴퓨터 인터페이스(HCI) 교육 등 시작품 제작을 위한 체계적인 교육을 제공한다.

경진대회에서 수상을 하기 위해서는 총 3번의 심사를 거친다. 첫 번째 서류심사에서는 아이디어의 창의성과 주제와의 부합정도를 주로 평가하며, 두 번째 발표심사에서는 구현 가능한 아이디어인지에 중점을 두고 평가를 한다. 마지막 본선대회 심사에서는 시작품 제작도의 완성도와 전체적인 디자인을 중점을 두고 평가한다.

‘웨어러블 컴퓨터 경진대회’는 대학생 특유의 참신한 아이디어를 바탕으로 하드웨어 구현 및 어플리케이션 제작, 외관 디자인까지 모든 영역에서 높은 점수를 받아야 하기 때문에, 한 분야를 전공한 대학생들끼리 팀을 만들기보다 다양한 전공을 가진 대학생들이 연합팀을 꾸린 팀들이 좋은 성적을 거둘 수 있다.

전국 대학교를 대상으로 매년 100팀 이상의 참가 접수가 이루어지며, 12년간 매년 개최되는 명실상부 IT 최고의 대회로 꼽힌다.

대회 참가는 국내 대학(원)생이면 누구나 접수 가능하며, 한 팀당 2인 이상 6인 이하로 팀을 이뤄 신청하면 된다. 참가접수는 홈페이지(http://www.ufcom.org)를 통해 가능하며, 올해 접수 기간은 오는 5월 31일까지다.

지난 대회 작품 소개

15 Degrees
가속도 센서를 이용한 모션인식 네비게이션 깔창

여행용 스마트 깔창은 깔창의 진동을 통해서
여행자와 인터랙션을 함으로써
미리 계획한 여행 경로를 자연스럽게 안내한다.
발로 모션을 인식함으로써 손이 자유롭고
시선이 스마트 폰이 아닌 풍경을 향한다.

PT블리
개성있고 기억에 남는 발표를 위한 PPT 제어복

현대 사회에서 중요한 커뮤니케이션 기능인
프리젠테이션의 효과를 극대화하기 위하여,
NUI 기술을 기반으로 하는 프리젠테이션 의상을
제작했다. 버튼으로 제어하는 기존의 기기보다
PT블리는 다양하고 화려한 퍼포먼스로
청중들의 이목을 사로잡을 수 있다.

Smart Helmet
오토바이를 안전하게 즐기도록 제작된 헬멧

오토바이를 안전하게 즐기도록 제작된 헬멧으로
빔 프로젝터로 HUD를 구현하여,
후방 화면을 헬멧 내부에 제공한다.
휴대폰 네비게이션, 카카오톡, 메시지 알림 등을
헬멧 내부에 제공한다.

옷이 4D
웨어러블 컴퓨터로 즐기는 4D 영화

어떤 감각도 쉴 틈 없는 4D 영화는 소비자들에게
새로운 경험과 재미를 줄 수 있는 상품이다.
'옷이 4D'는 언제 어디서든 입고
4D 영화를 즐길 수 있다. 블루투스 통신을
활용하여 옷으로 효과 정보를 전달하여
물, 바람, 진동, 연기 효과를 영화와 동시에 재생 시킨다.

웨어러블 보이
웨어러블 컴퓨팅을 이용한 1인칭 슈퍼마리오 게임

웨어러블 보이는 직관적인 일인칭 시점의
게임 디바이스이다. 웨어러블 보이는
기존 모션인식 게임기에 비하여 더욱 디테일한
모션 인식이 가능하며 사용자가 음성을 이용하여
게임을 제어할 수 있게 하였다.

행사 개요

- 행사명 : 2016 웨어러블 컴퓨터 경진대회
- 주 최 : KAIST 시스템설계응용연구센터
- 후 원 : 미래창조과학부, 삼성전자

대회 내용

- 지정공모 :
  주최 측이 제안한 주제 또는 미션에 맞는 웨어러블 컴퓨터 제안
  본선 진출팀은 시작품제작비 100만원을 지원받아 입는 컴퓨터를 제작

참가 자격

- 대학(2년제 포함)에 재학 중인 대학(원)생으로 구성된 2인 이상 6인 이하의 팀 (단, 패션/산업 디자인과 등 디자인과의 팀원이 있는 경우 7인까지 가능)

행사 주제

- 미션 : 아래 조건 중 1개 이상을 만족하는 웨어러블 시작품 제작

구 분	미 션
Culture	영화, 음악 등 문화생활을 즐기기 위한 웨어러블 컴퓨터
Education	학업관리, 유도 등 교육시장에서 사용될 웨어러블 컴퓨터
Wellness	건강예방, 치료, 관리 등 건강관리를 위한 웨어러블 컴퓨터

시상(안)

순 위	상 격	상 금
대상 1팀	미래창조과학부 장관상	500만원
최우수상 1팀	KAIST 총장상	200만원
우수상 1팀	삼성전자상	200만원
아이디어 특별상(중복가능)	미래창조과학부장관상	–

응모 일정 및 진행과정

- 접수 기간 : 3월 15일 ~ 5월 31일
- 진행 과정 : 참가 및 제안서 접수 ▶ 서류 및 발표 심사 ▶ 시작품 제작 ▶ 본선 대회

접수 방법

ⓐ 홈페이지 회원가입(www.ufcom.org)
ⓑ 팝업 또는 우측 베너 클릭 후 참가 신청
ⓒ 팝업 또는 자료실 게시판 클릭 후 아이디어 제안서 다운 / 작성
ⓓ 담당자 이메일로 접수
(E-mail. hn6139@kaist.ac.kr / 담당자 김현송 연구원)

문 의

Tel. 042)350-8932
E-mail. wcc@sdia.or.kr 또는 hn6139@kaist.ac.kr

IDEC Newsletter | 통권 제227호

발행일 2016년 4월 29일 **발행인** 박인철 **편집인** 김태욱, 남병규 **제작** 심원기획
기획 김하늘 **전화** 042) 350-8535 **팩스** 042) 350-8540 **홈페이지** http://www.idec.or.kr
E-mail kimsky1230@idec.or.kr **발행처** 반도체설계교육센터(IDEC)

반도체설계교육센터 사업은 산업통상자원부, 한국반도체산업협회, 반도체회사(삼성전자, SK하이닉스, 매그나칩반도체, 앰코테크놀로지코리아, 에이티세미콘)의 지원으로 수행되고 있습니다.