2025 ASSCC Review

한국과학기술원 바이오및뇌공학과 박사과정 석동열

Session 4 Wireless Powering & Stimulation Systems for Implants

이번 2025 ASSCC의 Session 4에는 Wireless Powering & Stimulation Systems for Implants 라는 주제로 총 4편의 논문이 발표되었다. 본 세션은 체내 이식형 전자기기 구동을 위한 무선 전력전송기술과 신경계조절용 전기자극기를 다루고 있다. 무선 전력전송 분야에서 2편(4-1, 4-2), 전기자극기 분야에서 2편(4-3, 4-4)이 게재되었다. 무선전력전송 분야에서는 초음파(ultrasonics), 자기전기효과(magnetoelectronic effect)와 같이 전기장 코일 방식의 대안으로 제시되는 무선전력기술의 기존 한계를 지적하고 극복하기 위한 다양한 방법이 제안되었으며, 전기자극기 분야에서는 이식형 신경 자극기의 활용분야를 넓히고 장기적 안정성을 확보하기 위한 자극기 설계 전략, 비침습적 뇌-심부 자극을 위한 시간-간섭 자극 방식의 자유도와 정밀도를 높이기 위한 집적회로 설계를 소개하였다.

#4-1 논문은 중국 동부과학기술대학교와 북경대학교의 공동연구로 초음파를 통한 체내 무선전력 전송 및 역-산란(backscattering)을 활용한 업-링크 데이터 전송기술의 한계를 극복하기 위한 방법을 제안하고 있다. 이 주제에 관련하여 기존에는 하나의 초음파 트랜스듀서에서 전력전송과 데이터 송신 기능을 동시에 수행할 수 있도록 하는 방법이 없었으므로 시분할(time-division) 방식의 트랜스듀서 활용 또는 전력전송 이외의 데이터 송신용 트랜스듀서를 추가하는 방법이 사용되었다. 저자는 이러한 기존 방식에서는 전력전달이 연속적이지 않으며, 데이터 전송속도가 높지 않고, 또한 추가적인 장치를 위한 공간, 전력이 필요하다는 제약이 있음을 지적하며, 초음파를 활용하는 무선 전력전송 기술에서도 연속적인 전력전달과 역-산란 데이터 전송이 동시에 가능하게 하는 구조를 제시한다.

가장 핵심적인 원리는 전력 수신부의 트랜스듀서와 연결된 코일로 가는 경로의 스위칭 주기를 조절하여, 하나의 트랜스듀서로 전력을 연속적으로 수신하면서 동시에 수신부의 입력 임피던스를 제어하는 것으로, 논문에서는 이를 통하여 역-산란 방식의 업-링크 데이터 전송을 가능하다는 것을 보여주었다. 이는 인덕터 충전 시간에 의해 트랜스듀서가 바라보는 평균 입력 임피던스가 결정되며, 이 값이 출력 부하의 변화와 상관이 없기 때문으로 이를 통하여 전력 전달과 데이터 전송이 연속적이고 동시에 가능해진다.

또한 저자들은 채널 상태 변화에 따른 통신 신뢰도를 확보하기 위해 업-링크 전송에 다중 변조 방식을 도입하고, 수신된 전력 레벨에 따라 변조 방식과 데이터 전송률을 적응적으로 선택하는 구조를 제안한다. 제안된 시스템은 BPSK, APSK, 4ASK 변조를 지원하며, 채널 상태가 양호한 경우 최대 300 kbps의 업-링크 데이터 전송률을 달성하면서도 비트 오류율(BER) 10^{-6} 수준의 신뢰도를 유지함을 실험적으로 보였다. 이러한 접근은 초음파 전력전송 환경에서 발생할 수 있는 채널 간 다양성에 대응하면서도, 기존 시분할 방식 대비 높은 유효 데이터율과 낮은 지연 시간을 가능하게 한다. 실험 결과, 약 5cm 깊이의 체내 환경을 모사한 조건에서 연속적인 전력 회수와 동시에 최대 약 192 μW 수준의 전력을 수신하면서 안정적인 업-링크 데이터 전송을 달성하였으며, 4ASK 변조 기준으로는 비트당 에너지 소모 6.3pJ/bit의 높은 에너지 효율을 기록하였다.

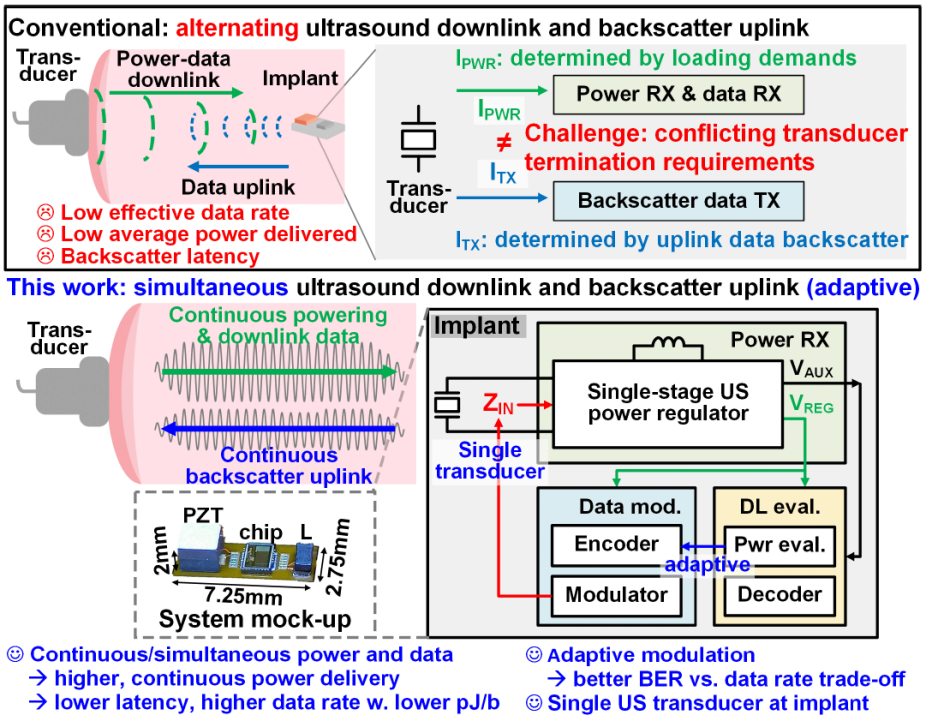


Fig. 1. Motivation and proposed simultaneous ultrasound downlink (power and data) and backscatter communication system.

[그림 1] 동시적 초음파 무선전력전달 및 데이터 통신 기술의 개념도

#4-4 논문은 한양대학교, KAIST 및 서울대학교가 참여한 공동연구로, 시간 간섭 자극(Temporal Interference Stimulation, TIS)을 다채널로 확장한 개념인 multi-TIS 의 구동 IC 를 제안한다. TIS 는 서로 근접한 주파수를 갖는 고주파 교류 전류를 중첩하여 심부 조직에서 저주파 포락선(envelope)을 형성함으로써, 표면 자극을 최소화하면서 심부 뇌 자극을 가능하게 하는 비침습적 신경조절 기법이다. 그러나, 기존의 TIS 시스템은 제한된 채널 수와 낮은 선형성, 채널 간 불일치로 인해 자극 공간 선택성이 충분하지 않으며, 보드 레벨 또는 단순 전류 미러 기반 회로에 의존함으로써 확장성과 정밀도에 한계가 있었다.

저자들은 이러한 문제를 해결하기 위해 고전압 증폭기 기반 전류 구동(source-sink) 구조를 채택한 12채널 multi-TIS 드라이버 IC를 제안한다. 제안된 구조는 기존 전류 미러 방식 대비 공정·전압·온도(PVT) 변화에 강인하며, 양방향 전류 구동을 통해 사인파 형태의 자극 신호를 보다 높은 선형도로 생성할 수 있다. 각 채널은 저전압 DAC 에서 생성된 정밀한 사인파 신호를 고전압 영역으로 증폭하여 전극에 인가함으로써, 다양한 부하 조건에서도 일정한 전류 자극을 유지할 수 있도록 설계되었다. 또한, 본 논문에서는 채널 간 이득 및 오프셋 불일치로 인해 발생하는 자극 왜곡을 보정하기 위한 3 단계 보정(calibration) 기법을 제안한다. 측정된 출력 파형을 기준으로 진폭 및 공통모드 오차를 추출하고, 이에 대응하는 보정 코드를 디지털적으로 적용함으로써 채널 간 불일치를 효과적으로 제거한다. 이를 통해 다채널 TIS 구동 시에도 포락선 신호의 왜곡을 최소화하고, 공간적으로 보다 정밀한 간섭 패턴 형성이 가능함을 보였다.

실험 결과, 제안된 IC 는 180 nm BCD 공정으로 제작되었으며, 최대 ±20 V 의 출력 전압 범위에서 채널당 최대 ±2 mA 의 자극 전류를 안정적으로 구동하였다. 15 kΩ 부하 조건에서 1 kHz 자극 시 SFDR 62 dB, SNDR 60 dB, THD 0.119%를 달성하였으며, 보정 이후 진폭 오차는 1% 미만으로 감소하였다. 또한 8 채널 multi-TIS 구성에서 단일 TIS 대비 약 25% 향상된 공간 선택성을 확인함으로써, 제안된 구조가 심부 뇌 영역을 보다 국소적으로 자극할 수 있음을 실험적으로 입증하였다.

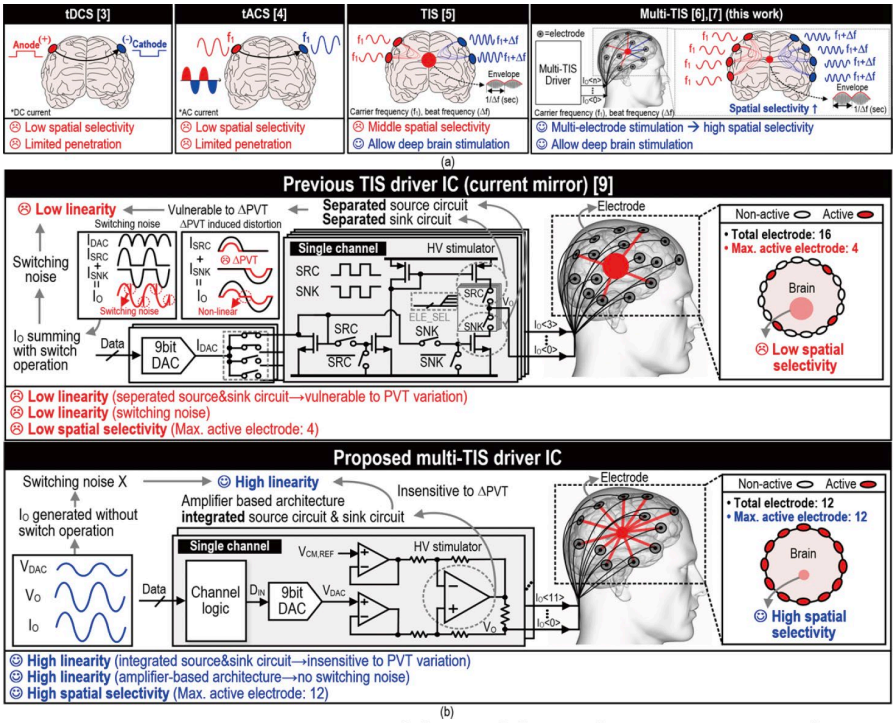


Fig. 1. (a) principles of tDCS, tACS, TIS, and multi-TIS, (b) comparison between previous and proposed TIS driver IC.

[그림 2] 제안된 다중 시간-간섭 자극기(multi-TIS) 구동회로의 개념도

저자정보

석동열 박사과정 대학원생

- 소속 : 한국과학기술원
- 연구분야 : 바이오메디컬 응용 회로설계(센서 및 신호처리)
- 이메일 : sukd10@kaist.ac.kr

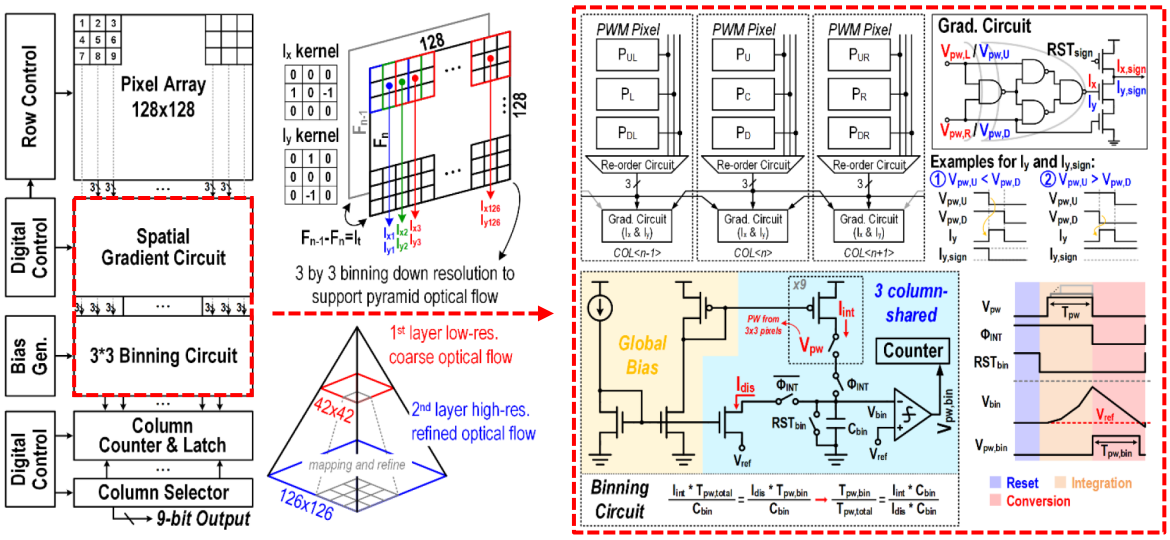
A-SSCC 2025 Review

울산과학기술원 전기및전자공학부 석박통합과정 홍기업

Session 16 Visual Interactive System

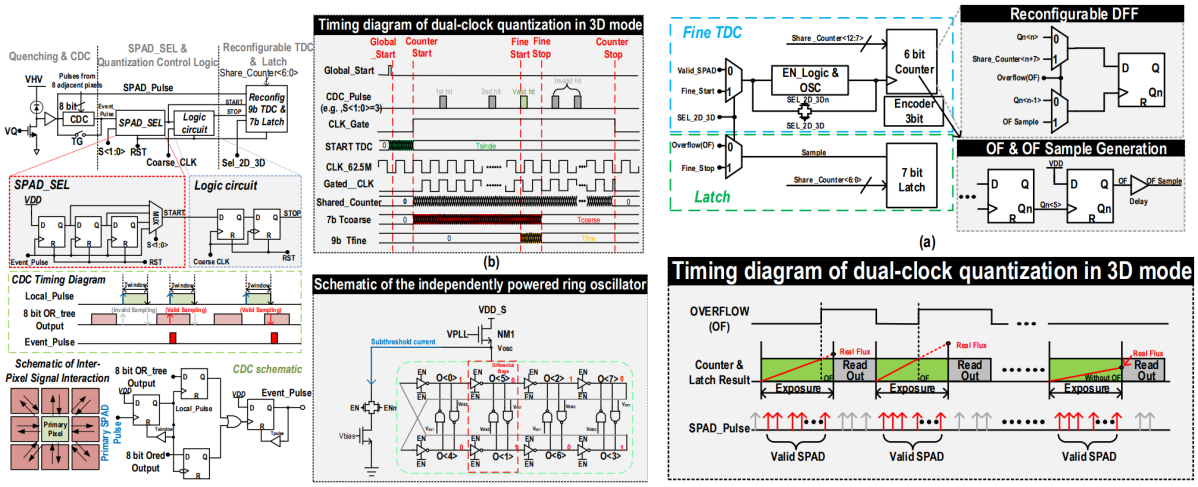
올해 ASSCC session 16에는 3개 image sensor 논문과 1개의 capacitive 터치센서 논문이 소개되었다. 이미지센서 분야에서는 구체적으로 PIS(processing-in-sensor), LiDAR, SPAD-PPD hybrid image sensor가 소개되었으며 현재 가장 활발히 연구되고있는 분야의 논문들이다. 각 논문은 연산 에너지 효율 향상(16.1), background immunity 향상(16.2), 픽셀 구조 소형화 및 dynamic range 향상(16.3)을 목표로한 센서를 제안한다.

#16-1 National Tsing Hua University에서 발표한 논문으로 128×128 dual-resolution processing-in-sensor (PIS) 구조를 제안하며, optical-flow 기반 motion processing이 핵심이다. 픽셀은 기존에 같은 그룹에서 발표되었던 6T1C PWM 구조로 구성되어 있으며, 단일 프레임 내에서 raw image, temporal gradient, spatial gradient를 동시에 출력할 수 있도록 한다. Spatial gradient 연산은 컬럼 단에 구현된 low-power, area-efficient combinational logic을 통해 수행하며 기존의 OPAMP-based 혹은 adder-based subtractor 대비 높은 에너지 효율을 달성한다. 또한 3×3 binning 회로를 추가하여 저해상도 optical-flow pyramid 입력을 직접 센서에서 생성할 수 있어, 외부 프로세서의 연산 부담을 줄일 수 있다. 따라서 제안된 센서는 9-bit raw image, temporal/spatial gradient, 3×3 binning을 모두 지원하면서도 30fps에서 198.44 μW의 매우 낮은 전력을 달성한다.



[그림 1] 전체 chip architecture(좌)와 제안하는 spatial gradient 및 binning 회로

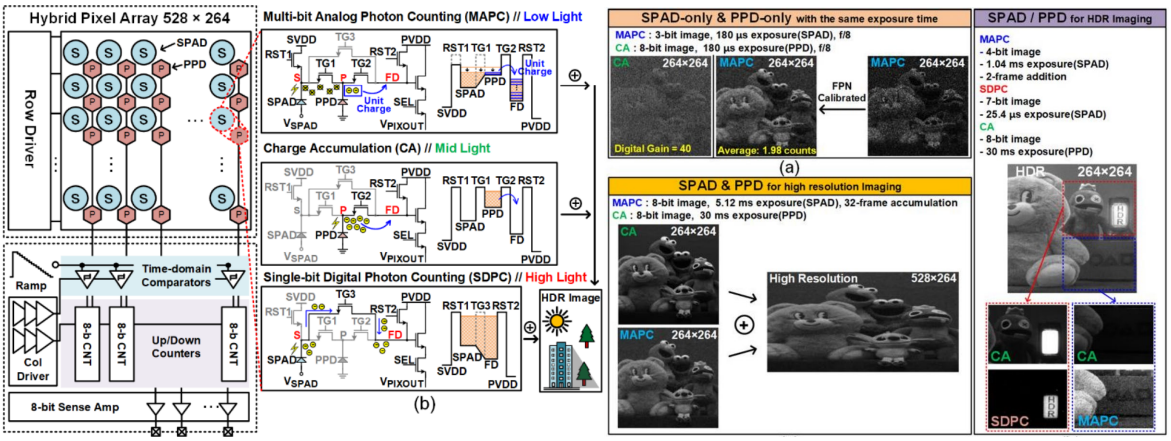
#16-2는 Xidian University에서 제안한 flash LiDAR sensor이다. 본 논문은 픽셀 구조를 재구성하여 high dynamic range 2D intensity와 dToF기반 3D depth를 sensing할 수 있는 센서를 디자인하였다. 본 센서는 전체 픽셀 어레이가 동시에 픽셀별 photon의 time of flight를 digitize 하는 flash type dToF sensor이다. 기존 dToF센서의 challenge였던 background에 의한 TDC 및 SPAD pile up issue를 CDC(coincidence detection circuit)와 first-last hit signal selection으로 해결하였다. 또한 3D mode에서 TDC로 활용하던 counter를 2D mode에서는 photon counting에 사용하여 2D sensing이 가능하게 하였다. 더 나아가 2D intensity dynamic range 확장을 위해 TTS(time to saturation) 방식을 이용하여 counter가 정해진 counter depth를 초과하였을 때의 시간을 픽셀에 저장하여 119dB에 달하는 dynamic range를 달성하였다.



[그림 1] 3D mode 동작 timing diagram 및 CDC, first-last hit detection circuit(좌),

HDR 2D mode 동작의 operational concept과 timing diagram(우)

#16-3는 Sungkyunkwan University에서 제안한 HDR 2D sensor이다. 본 논문은 인간 눈에 있는 간상세포와 원추세포를 모방한 하이브리드 픽셀 어레이를 디자인하였다. 각 세포는 각각 SPAD 와 PPD로 구현하였으며 광자 감지 민감도가 높은 SPAD와 낮은 PPD소자를 결합함으로써 넓은 조도 상황에서 능동적으로 빛을 감지할 수 있게 하였다. SPAD소자는 높은 광자 감지 민감도로 인해 일반적으로 저조도 센싱에 매우 탁월하나 photon counting counter 구조가 PPD기반 픽셀보다 비교적 복잡하다는 단점이 있다. 본 논문에서는 해당 픽셀 구조를 4개 미만의 transistor로 간소화하였으며 photon counting 필요한 charge transfer를 PPD를 이용하여 효율적으로 구현하였다. 이를 통해 110nm BSI process에서 18.295μm × 14.5 μm라는 비교적 작은 픽셀 크기를 달성할 수 있었으며, SPAD 및 PPD response를 결합함으로써 109dB라는 큰 dynamic range를 달성하였다.



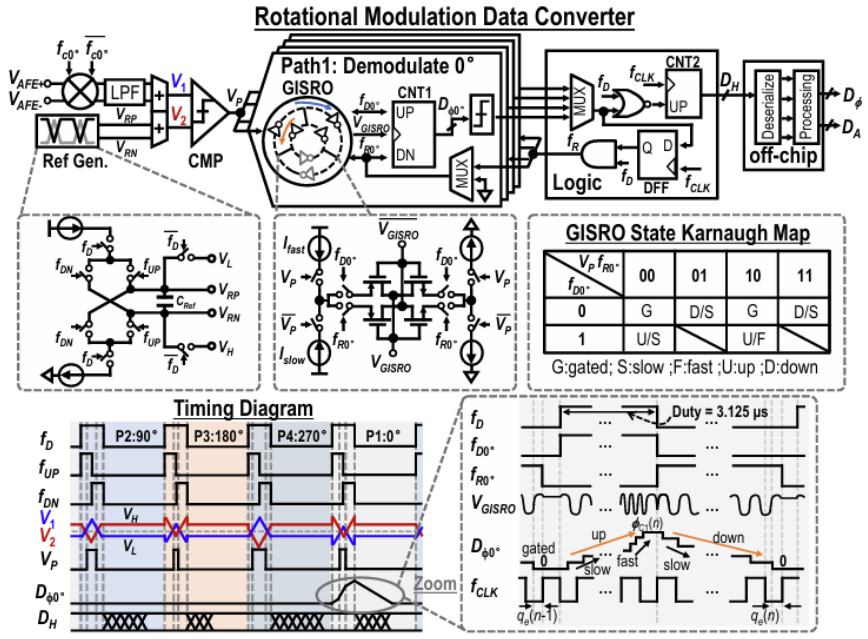
[그림 2] 센서 아키텍처 및 하이브리드 픽셀 operational concept (좌),

본 센서로 획득된 HDR 및 고해상도 이미지 (우)

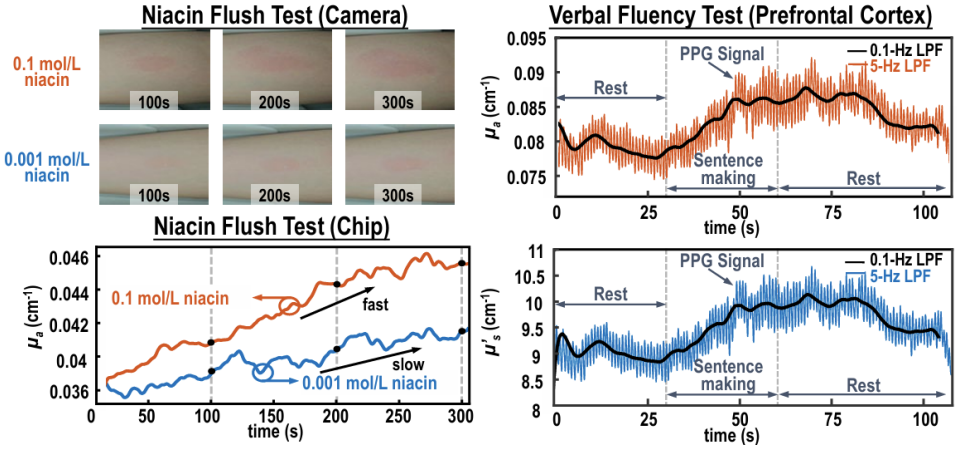
Session 20 Circuits for Cognitive and Physiological Interfaces

ASSCC 2025의 Session 20은 'Circuits for Cognitive and Physiological Interfaces' 주제로 총 5편의 논문이 발표되었다. 그 중 Processor, FD-NIRS, Neural recording System-on-Probe(SoP)에 대한 3편의 논문을 살펴보고자 한다.

#20-2 fNIRS는 웨어러블 구성과 비침습 방식으로 실시간 뇌 활성도를 관찰할 수 있어, 정신의학 연구에서 주목받고 있다. Shanghai Jiao Tong 대학에서 발표한 본 논문은 dynamic TIA 기반 저전력 아키텍처와 APD DC servo loop, 4-phase 샘플링 기법을 통해 1ps 미만의 고해상도 ToF FD-NIRS 시스템을 제안하였다. 제안된 Rotational Modulation Data Converter(RMDC) 구조는 하나의 신호 주기 내 4개 지점 샘플링을 통해 과잉결정 행렬을 형성하여 별도의 보정없이 오프셋에 강인한 신호 복원을 수행하며, Differential difference PWM Frontend를 통해 비교기의 zero-crossing 동작으로 선형성을 확보하였다. 또한, GISRO 기반 위상 도메인 듀얼 슬로프 data converter는 gating시의 freeze 특성을 활용한 1차 noise shaping으로 높은 분해능을 달성한다. 이를 통해 14.6mW의 저전력으로 0.93ps ToF 분해능을 달성하였고, In-vitro 실험에서 흡수·감소 산란계수의 최대 오차 3% 미만으로 기존 기술 대비 우수한 검출 정확도를 입증했다.

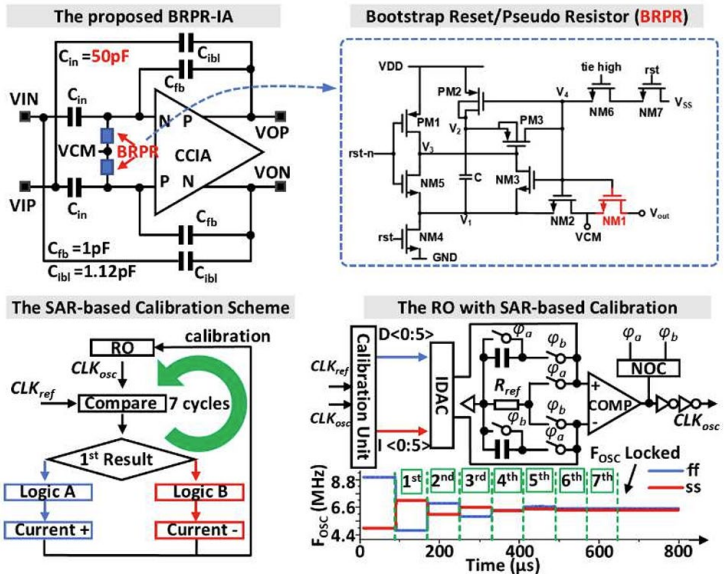


[그림 1] 고해상도 FD-NIRS를 위해 제안된 Data Converter 회로도 및 동작 원리

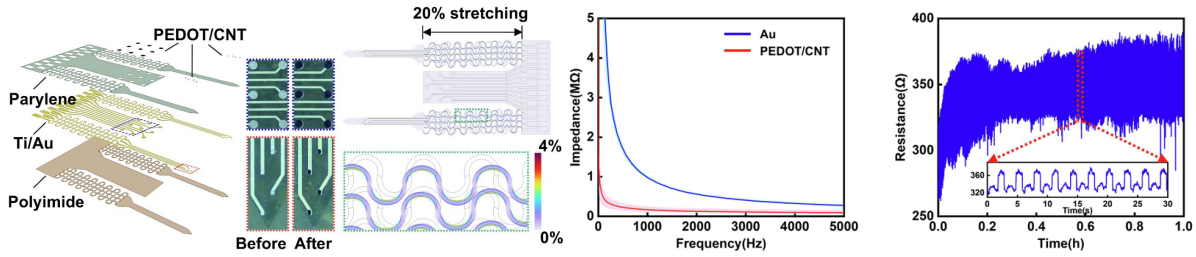


[그림 2] Niacin 홍조 반응(왼쪽)과 언어유창성 검사(오른쪽) 시연 결과

#20-4 Guangdong Institute of Intelligence Science and Technology에서 제안하는 Neural Miner는 System-on-Probe(SoP) 구조의 16채널 신경 기록 시스템으로, 기록칩과 신축성 프로브을 단일 소형 패키지로 통합하여 다중 뇌 영역을 최소 침습으로 동시에 기록한다. 제안하는 Bootstrap Reset/Pseudo Resistors(BRPR-IA) 구조는 대면적 입력 트랜지스터와 50pF 캡을 통해 1/f 노이즈를 억제하고, 리셋 스위치와 pseudo-저항을 결합한 BRPR 구조를 도입하여 기존의 dead zone 문제를 없애고, TΩ급 고임피던스를 안정적으로 유지하도록 한다. 또한 on-chip SAR 기반 보정이 적용된 closed-loop RO를 통해 IRN 1.18μVrms, CMRR>110dB의 신호 무결성을 확보하였다. PEDOT/CNT 전극(전극 사이즈 : 35x35μm^2)과 서펜타인 구조 프로브를 적용하여 낮은 전극 임피던스와 기계적 유연성을 동시에 구현하였다. 측정 결과 0.12mm^3/ch의 소형 폼팩터에서 ECoG, LFP, AP를 In-vivo로 기록하여 고집적·저침습 신경 인터페이스로서의 가능성을 입증하였다.



[그림 3] 제안된 BRPR-IA 회로(상단)와 SAR 기반 보정의 RO 회로(하단)



[그림 4] 신축성 프로브 구조(왼쪽)와 프로브의 임피던스 측정결과(오른쪽)

저자정보

홍기업 석박사통합과정 대학원생

- 소속 : 울산과학기술원
- 연구분야 : 센서디자인, 혼성회로설계
- 이메일 : slsnsep357@unist.ac.kr
- 홈페이지 : https://sites.google.com/view/bias-sogang/home

A-SSCC 2025 Review

고려대학교 전기전자공학과 박사과정 한창우

Session 24: Advanced Circuits for Memory and Sensing

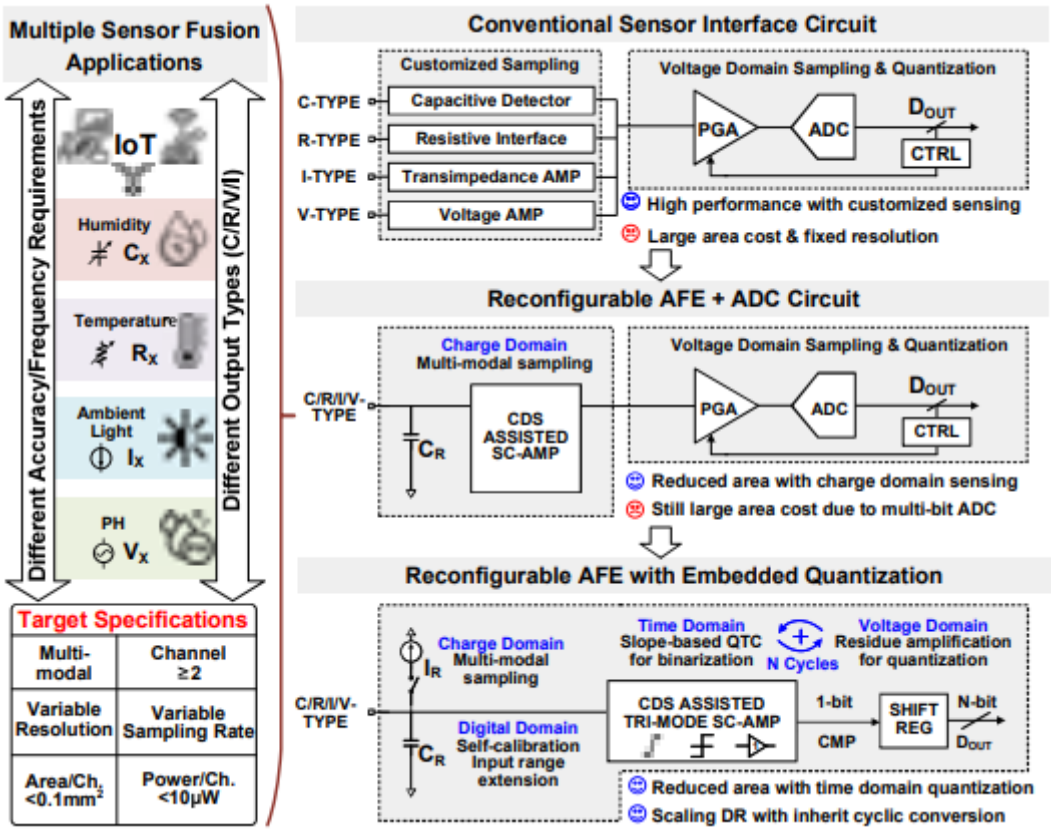
이번 A-SSCC 2025 Session 24에서는 차세대 메모리 및 센싱 회로 기술을 주제로 총 4편의 논문이 발표되었다. 본 세션은 3D DRAM 및 멀티모달 센서 인터페이스를 중심으로, 고집적·저전력 시스템 구현을 위한 아날로그 회로 설계를 다룬다. 특히 공정·전압·온도(PVT) 변화에 강인한 회로 구조를 통해 면적 및 전력 효율을 개선하는 설계 전략이 공통적으로 제시되었다. 본 리뷰에서는 Session 24 중 3D DRAM과 멀티모달 센서 인터페이스 기술을 다룬 두 편의 논문을 중심으로 살펴보고자 한다.

#24-2 본 논문은 Shanghai Jiao Tong University에서 발표한 연구로, 전압·전류·저항·커패시턴스(V/I/R/C) 신호를 하나의 회로에서 처리할 수 있는 멀티모달 스위치드-캐패시터(SC) 센서 인터페이스를 제안한다. IoT 및 센서 응용 환경에서는 다양한 물리량을 동시에 측정해야 하나, 기존 센서 인터페이스는 신호 종류별로 개별 아날로그 프론트엔드(AFE)와 ADC를 필요로 하여 면적과 전력 소모가 증가하는 한계가 있었다.

이를 해결하기 위해 본 논문에서는 모든 입력 신호를 전하(charge) 도메인으로 통합하고, 이를 시간 영역 기반 Charge-to-Time Conversion(QTC) 방식으로 양자화하는 새로운 구조를 제안한다. 제안된 회로에서는 V/I/R/C 입력 신호를 단일 커패시터(CR)에 샘플링한 뒤, CDS(Correlated Double Sampling)가 적용된 SC 증폭기를 통해 신호를 증폭하며, 이후 동일한 증폭기를 QTC 동작에 재사용하여 별도의 ADC 없이 디지털 출력을 생성한다.

특히 변환 과정에서 발생하는 residue 전하를 증폭하여 다음 변환 사이클의 입력으로 사용하는 cyclic residue amplification 구조를 도입함으로써, 고해상도 동작 시 변환 사이클 수가 급격히 증가하는 문제를 효과적으로 완화하였다. 또한 시간 영역 양자화의 특성을 활용한 digital self-calibration 기법을 적용하여 공정·전압·온도(PVT) 변화 및 비교기 지연에 따른 오차를 최소화하였다.

측정 결과, 제안된 회로는 55 nm CMOS 공정에서 구현되었으며, 채널당 약 0.015 mm^2의 면적, 6.4 μW의 저전력 소모, 그리고 V-mode에서 SNDR 38.3 dB의 성능을 달성하였다. 또한 C-mode에서는 self-calibration을 통해 최대 1 nF까지 입력 범위 확장이 가능함을 실험적으로 검증하였다. 본 논문은 하나의 SC 증폭기를 센싱과 양자화에 동시에 활용함으로써 멀티모달 센서 인터페이스의 집적도와 전력 효율을 크게 향상시킨 설계로, 저전력 IoT 센서 시스템에 적합한 실용적인 솔루션을 제시한다.



[그림 1] 기존 센서 인터페이스 회로와 제안된 재구성형 스위치드-캐패시터 기반 멀티모달 센서 인터페이스 구조

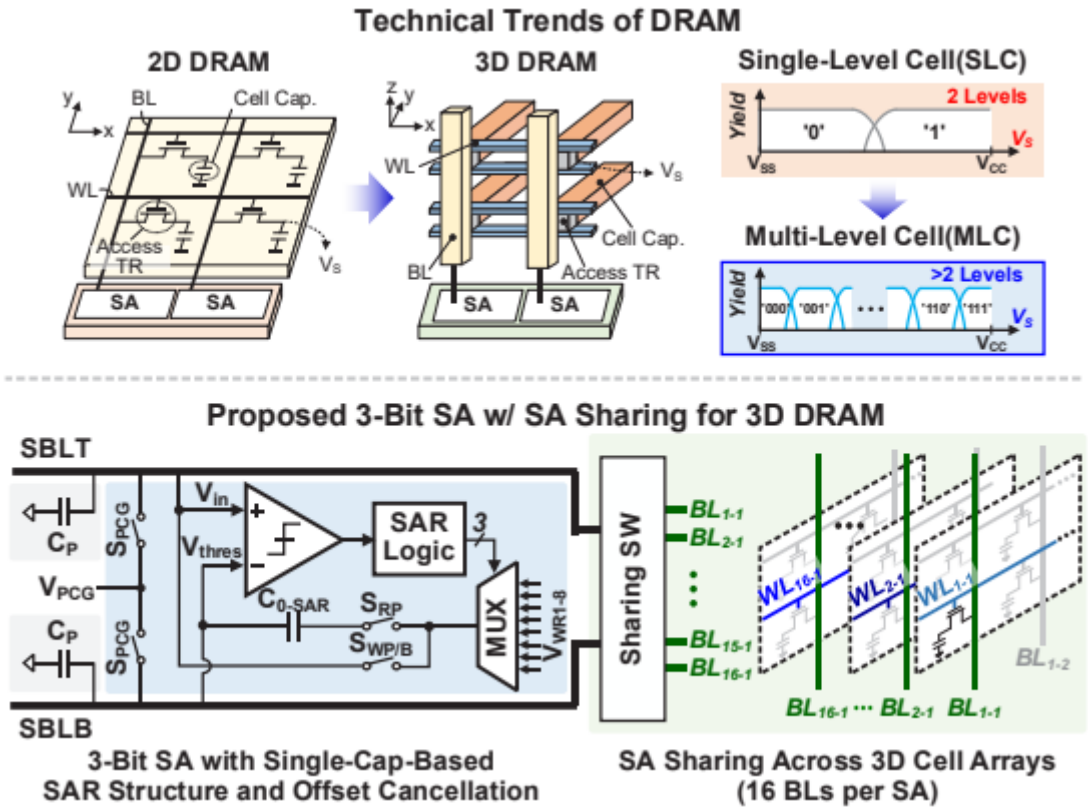
#24-3 본 논문은 KAIST에서 발표한 연구로, 3D DRAM 환경에서 멀티레벨 셀(MLC) 구현을 위한 3-bit sense amplifier(SA) 구조를 제안한다. 3D DRAM은 수직 적층 구조를 통해 고집적 메모리 구현이 가능하나, 셀 캐패시턴스 감소와 비트라인 기생 성분 증가로 인해 기존 단일 비트 SA 구조만으로는 안정적인 MLC 동작에 한계가 있다.

이를 해결하기 위해 본 논문에서는 단일 커패시터 기반 SAR ADC 구조를 적용한 3-bit SA를 제안하며, SA 내부에 offset cancellation 기법을 결합하여 공정 및 소자 불균일성에 따른 오프셋 문제를 완화하였다. 제안된 SA는 셀 전압을 직접 비교하는 대신, charge-domain 기반의 비교 및 디지털 변환 방식을 사용함으로써 고정밀 다중 비트 판별이 가능하도록 설계되었다.

또한 3D DRAM의 구조적 특성을 고려하여 SA sharing 기법을 도입함으로써, 하나의 SA가 여러 비트라인을 공유하면서도 안정적인 판독이 가능함을 보였다. 이는 기존 SA sharing 방식에서 문제로 지적되던 순차적 복원에 따른 타이밍 오버헤드를 제거하고, 3D DRAM 환경에 최적화된 구조임을 실험적으로 검증하였다.

측정 결과, 제안된 3-bit SA는 28 nm CMOS 공정에서 구현되었으며, 기존 구조 대비

SA 오프셋 분산을 크게 감소시키고, 낮은 공급 전압 조건에서도 안정적인 MLC 동작이 가능함을 확인하였다. 본 논문은 3D DRAM에서 요구되는 고집적·고정밀 판독을 회로 수준에서 실현한 연구로, 향후 고용량 3D DRAM 시스템에 적용 가능한 실질적인 SA 설계 방향을 제시한다.



[그림 2] 3D DRAM 기술 동향 및 SA 공유 구조를 적용한 3-bit SAR 기반 센스 앰프 구조

저자정보

한창우 박사과정 대학원생

- 소속 : 고려대학교 전기전자공학과
- 연구분야 : 차세대 반도체 소자 및 회로
- 이메일 : cwoo0105@naver.com
- 홈페이지 : https://sites.google.com/view/kudclab

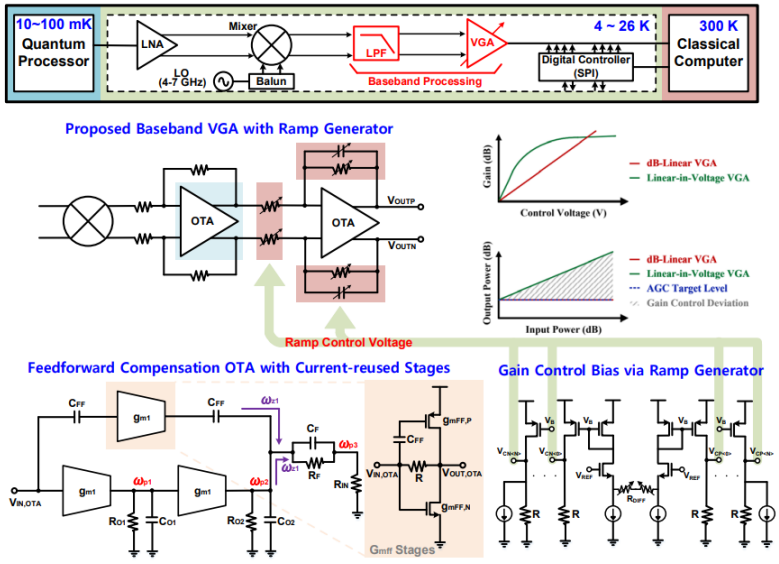
A-SSCC 2025 Review

포항공과대학교 반도체대학원 박사과정 박은빈

Session 26 Circuits and Systems for Quantum and Security

2025 IEEE A-SSCC의 Session 26에서는 Cryogenic CMOS 기반 양자 컴퓨팅 인터페이스, 센서 보안 아키텍처, 그리고 고성능 암호 가속기라는 세 가지 핵심 연구 축을 중심으로 총 네 편의 논문이 발표되었다. 최근 반도체와 컴퓨팅 분야에서는 양자 프로세서와의 근거리 통합을 가능하게 하는 Cryo-CMOS 기술, 그리고 양자 이후 시대를 대비한 Post-Quantum Cryptography(PQC) 연산 가속기와 같은 연구가 빠르게 확대되고 있다. Session 26의 논문들은 이러한 기술적 변화 흐름을 반영하며, 미래의 고신뢰·고효율 컴퓨팅 시스템을 구성하기 위한 회로 및 아키텍처 수준의 혁신적인 접근법들을 제시하고 있다.

#26-1 논문에서는 4–7 GHz 대역을 지원하며 낮은 노이즈와 높은 선형성을 제공하는 cryogenic CMOS 기반 다중 큐비트 읽기(read-out) 회로를 제안하였다. 양자컴퓨팅 시스템이 대규모로 확장되기 위해서는 수백에서 수천 개의 큐비트를 수십 마이크로초 내에 빠르게 측정해야 하는데, 기존 실온(RT) 기반 구조는 케이블 증가로 인한 열부하, 노이즈 유입, 복잡한 배선 문제 때문에 확장성이 제한적이었다. 본 논문은 이러한 문제를 해결하기 위해 극저온 환경에서 동작하는 단일칩 cryo-CMOS ROIC를 설계하였으며, 이를 통해 다중 큐비트 read-out을 위한 저잡음·고구성 효율의 RF 경로를 제공한다. 제안된 회로는 48 K noise temperature, 52.3 dB SFDR, 4–7 GHz 대역 지원을 달성하여 기존 cryogenic 인터페이스 대비 성능과 실용성을 크게 향상시켰다.
본 논문은 먼저 극저온에서 발생하는 트랜지스터 gm 변화 및 flicker noise 증가 문제를 해결하기 위해 Transformer 기반 Dual Noise-Canceling LNA 구조를 적용하였다. CG/CS 결합 구조를 변압기 기반 피드백 경로와 함께 사용함으로써 cryogenic 환경에서 크게 변동하는 잡음 성분을 효과적으로 상쇄하고, 기존 대비 44% 개선된 NF를 달성하였다. 또한, mixer 단계에서는 cryogenic 환경에서 flicker noise가 더욱 심각해지는 문제를 해결하기 위해 Transformer-coupled Current-Bleeding Mixer를 제안하였다. Current Bleeding(CB) 구조는 flicker noise를 줄이는 데 유리하지만 thermal noise를 증가시키는 단점이 있는데, 본 논문은 transformer를 이용해 이러한 thermal noise 증가를 억제하여 넓은 대역폭과 높은 변환이득을 동시에 확보하였다. 여기에 dB-linear VGA와 253 MHz IF 대역폭을 지원하는 이득 제어 블록을 추가하여 multi-qubit read-out에서 필요한 정밀 이득 조절과 넓은 IF 처리 범위를 실현하였다.



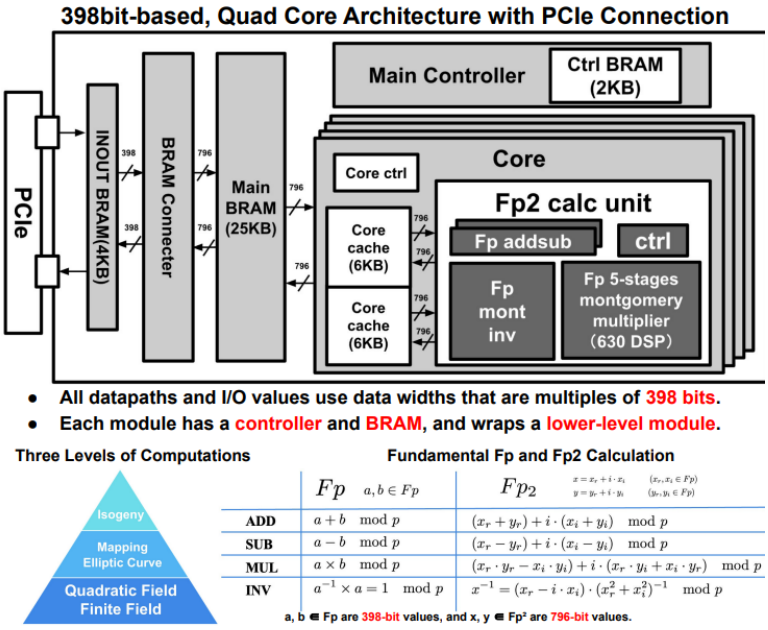
[그림 1] 제안된 cryo-CMOS 기반 multi-qubit read-out RF 수신기 구조

측정 결과, 제안된 cryo-CMOS ROIC는 극저온 환경에서도 안정적으로 동작하며, multi-qubit read-out에 필요한 고선형성·저잡음 성능을 충족함을 입증하였다. 또한 단일칩 구조를 통해 기존 실온 기반 측정 시스템이 요구하던 복잡한 배선을 줄이고, 열부하를 감소시켜 대규모 큐비트 확장성 측면에서도 중요한 장점을 확보하였다. 본 논문은 cryogenic RF 회로의 안정성, 노이즈 특성 개선, 다중 큐비트 지원 능력을 종합적으로 향상시킴으로써 대규모 양자컴퓨팅 시스템을 위한 실용적이고 확장 가능한 read-out 인터페이스 설계 방향을 제시한 연구로 평가될 수 있다.

#26-3 논문에서는 398bit (2,2)-isogeny 기반 Post-Quantum Cryptography(PQC)를 고속 처리하기 위한 FPGA 가속기 아키텍처를 제안하며, 기존 소프트웨어 중심 isogeny 연산의 병목을 해결하는 새로운 하드웨어 접근 방식을 제시하였다. Isogeny 기반 암호는 짧은 키 길이라는 장점에도 불구하고 대규모 정수 연산과 복잡한 곡선 변환 과정으로 인해 계산 비용이 매우 크다는 문제가 있었다. 본 논문은 이러한 한계를 극복하기 위해 398bit 데이터 경로 기반의 4-코어 병렬 FPGA 구조를 도입하여 연산 병렬성과 메모리 활용 효율을 극대화하였다. 특히, 기존 구현들이 직면했던 메모리 접근량 폭증과 낮은 스루풋 문제를 해결하고자, 각 연산 단계의 데이터 생애(lifetime)를 분석하여 메모리 공간을 재할당하는 정적 캐시 최적화 기법을 적용하였으며, 이를 통해 기존 대비 약 75%의 BRAM 사용량을 절감하였다.

본 논문은 또한 하드웨어에서 가장 큰 연산 비용을 차지하는 모듈러 곱셈을 가속하기 위해 5-stage 파이프라인 Montgomery multiplier를 설계하였다. 398bit 곱셈을 64bit DSP 블록으로 분해해 매핑함으로써 LUT 기반 구현 대비 최대 8.5배 높은 동작 속도를 확보하였다. Isogeny 체인에서 자주 등장하는 DBL·MAP·FJTJ 연산의 구조적 병렬성을 분석하여 핵심 함수들을 효과적으로 스케줄링한 점도 중요한 기여다. 특히, DBL과 MAP은 상호 독

립적으로 병렬 수행이 가능하며, 이를 최대 4코어 수준으로 동시에 처리해 전체 isogeny 체인의 실행 횟수를 최소화하였다. 이러한 최적화된 경로는 SageMath 기반 소프트웨어 구현 대비 총 연산 비용을 약 9% 추가 절감하는 성능 향상을 가져왔다.



[그림 1] 제안된 4-코어 FPGA 기반 isogeny 연산 가속기 구조

측정 결과, 제안된 FPGA 가속기는 호스트 CPU 대비 최대 87%의 지연 시간 단축(59.6 ms)을 달성했으며, 기존 C/GMP 기반 단일 스레드 구현과 비교해 현저히 빠른 처리 속도를 보여주었다. 특히, FESTA·QFESTA 등 최신 isogeny 기반 암호 스킴에서 반복적으로 등장하는 (2,2)-isogeny 연산을 효율적으로 가속함으로써, 향후 PQC 표준화 과정에서 isogeny 계열 암호의 실용화를 뒷받침할 수 있는 중요한 하드웨어적 가능성을 제시한다. 본 연구는 고비용 정수 연산, 메모리 병목, 연산 스케줄링 문제를 종합적으로 해결함으로써 차세대 보안 시스템을 위한 고성능 PQC 가속기 설계에서 의미 있는 진전을 보여준다.

저자정보

박은빈 박사과정 대학원생

- 소속 : 포항공과대학교
- 연구분야 : HW-SW co-optimization 및 양자오류정정부호
- 이메일 : eunbin@postech.ac.kr, eunbin.epiclab@gmail.com
- 홈페이지 : https://sites.google.com/view/epiclab/member/ebpark