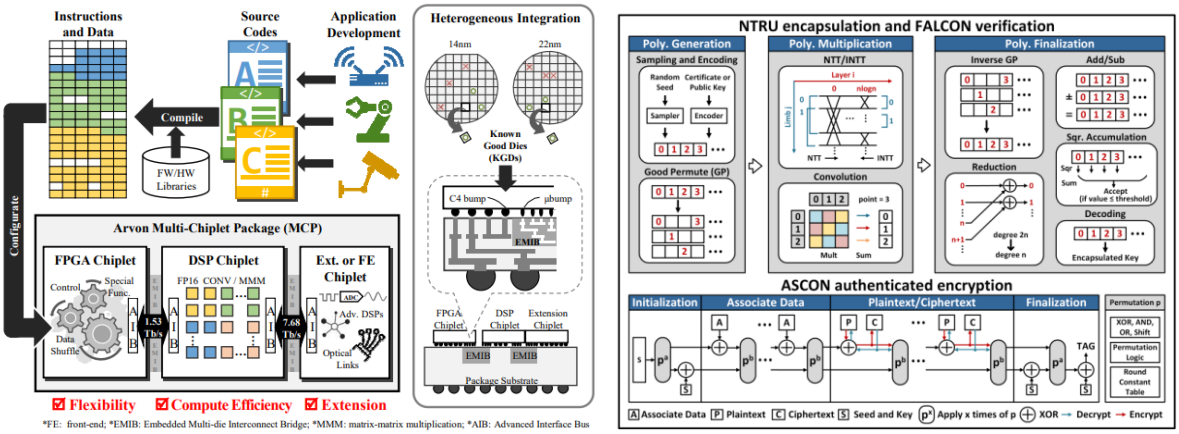
2023 IEEE VLSI Review

서울대학교 전기정보공학부 박사과정 박현준

Session 7 Digital Systems



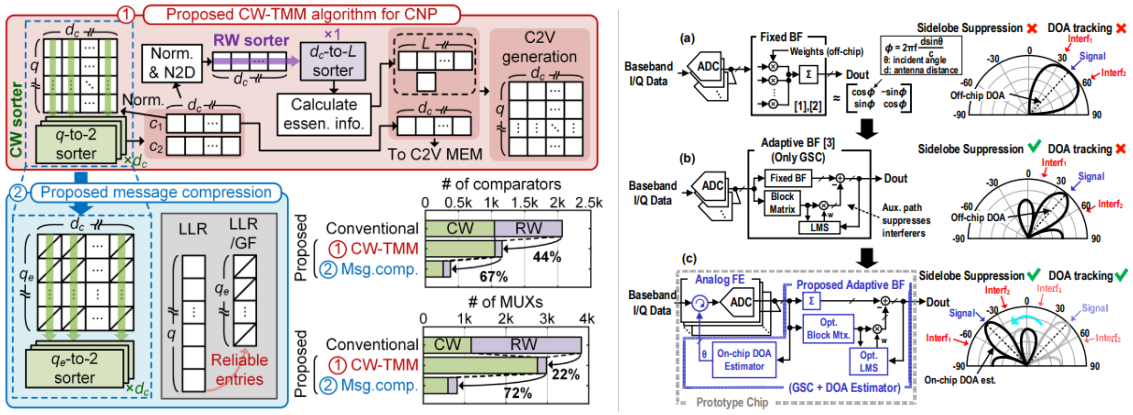
[그림 1] (좌) 7-1 (우) 7-2

#7-1 이 논문에서 제안하는 Arvon은 14nm FPGA 칩과 두 개의 22nm DSP 칩을 결합한 이종 시스템 패키지(SiP)다. 이는 Embedded Multi-die Interconnect Bridges (EMIBs)를 통해 통합되며, 최대 7.68Tbps의 AIB 2.0 인터페이스를 통해 통신이 이뤄진다. Arvon은 신경망(NN)에서 통신 처리까지 다양한 작업을 지원하며, DSP 칩 당 최대 4.14TFLOPS의 성능을 달성한다. DSP가 주요 커널 기능을 처리하고 FPGA가 데이터 정렬 및 특수 기능을 지원하여 유연성과 효율성을 극대화하여 대역폭 밀도와 에너지 효율성을 향상시켜 NN 및 통신 작업에 대해 뛰어난 성능을 제공할 수 있다.

#7-2 이 논문은 40nm CMOS 공정에서 제작된 세계 최초의 Post 양자 하이브리드 암호(PQC) SoC를 소개하며, 800Mbps의 처리량을 달성하고 원격 신경 인터페이싱을 위해 4.8mW의 전력을 소비한다. 이 SoC는 PQC와 경량 암호화(LWC)를 결합하여 양자 레벨의 공격을 방어하며 데이터 암호화의 복잡성을 줄인다. 특정 최적화 전략들의 사용으로, 기존 설계에 비해 더 높은 면적 효율과 에너지 효율도 보여준다. 이는 높은 보안이 요구되거나 고속의 원격 신경 인터페이싱이 필요한 애플리케이션에 유망한 솔루션이 될 수 있

다.

#7-3 이 논문은 일차원 및 이차원 결합 부분 미분 방정식(PDEs)을 푸는 데 사용되는 디지털 비트-직렬 컴퓨팅 가속기를 소개한다. 20x10 완전 병렬 처리 요소(PE) 배열로 최소한의 에너지/면적 오버헤드로 높은 병렬 처리 능력을 갖추었다. 이로 인해 기존 CPU 및 GPU 아키텍쳐보다 더 나은 에너지 효율성과 성능 향상을 제시하여 다양한 응용분야의 PDEs 해법에 도움을 줄 수 있다.



[그림 2] (좌) 7-4 (우) 7-5

#7-4 이 논문은 비바이너리 저밀도 패리티-체크 (NB-LDPC) 디코더의 효율적 구현을 위해 컬럼 기반의 트렐리스 민-맥스 (CW-TMM) 알고리즘을 제시한다. 이 방식은 TMM 방식의 Align 연산 비용을 크게 줄이면서도 오류 수정 능력을 희생하지 않는다. 또한, 메시지 압축이 디코더에 적용되어 긴 NB-LDPC 코드에 대한 필요 메모리를 최소화한다. 회로 수준의 최적화를 통해 불필요한 연산 유닛을 제거하여, 28nm CMOS 공정에서의 프로토타입 디코더는 디코딩 복잡성과 온칩 메모리 크기를 각각 63%와 54% 줄여 2.35 Gb/s/mm2의 효율을 달성했다.

#7-5 이 논문은 65nm 밀리미터파 베이스밴드 디지털 빔포머를 소개하며, 이 빔포머는 적응형 사이드로브 캔슬러와 DOA 추정을 통합한다. DOA 추정을 기반으로 위상 회전기의 가중치를 선제적으로 조정하여 사이드로브 취소 루프를 간소화한다. 추정(ESPRIT DOA)의 복잡도를 최소화하기 위해 CORDIC 기반 QR-반복을 사용해 행렬 계산도 피할 수 있다. 전체 시스템은 0.64mm^2의 영역을 차지하며, 100MHz에서 60mW를 소모하고, DOA 추정과 함께 600 pJ/symbol의 에너지 효율을 달성한다.

Session 12 Digital Building Blocks

#12-1 이 논문은 fully 합성 가능한 True Random Number Generator (TRNG)를 소개하며, 이 TRNG는 링 발진기 (RO)에서의 에지 추적을 기반으로 한다. 여러 에지가 2-Edge even-stage RO(2E-RO)에 주입될 때, 한 에지가 다른 에지를 추적하고 충돌하는 데 걸리는 시간, 즉 Cycles-to-Chase (CTC)가 엔트로피 소스로 사용된다. 이는 매우 고품질의 엔트로피 소스이고, 고속 작동을 위해 자동 자체 보정 루프를 갖춘 구성 가능한 RO를 제안하여, 100.8Mbps까지의 무작위 비트 생성 속도를 달성하면서 모든 NIST 테스트를 후처리 없이 통과한다.

#12-2 이 논문은 4nm CMOS에서 구축된 개인 정보 보호 상호 인증(PPMA) 가속기를 소개한다. 128비트의 강력한 보안 기능(PUF)과 AES-128 라운드 하드웨어를 사용하는 double-connection 암호 마이크로아키텍처가 통합되어 부수 채널 공격(SCA) 및 머신러닝(ML) 모델링에 강한 저항력을 보였으며, 안전한 무선 센서 네트워크를 보장한다. 가속기의 설계는 암호화를 위해 실시간으로 생성된 nonces를 사용하여 서비스 거부 공격에 대한 저항력을 향상시키며, 1번의 인증당 3nJ의 뛰어난 에너지 효율성을 보인다.

#12-3 이 논문에서는 새로운 다중 수준(2 bits/bitcell) SRAM PUF를 소개하며, 이를 통해 비트셀 변경 없이 저장 용량을 초과하는 PUF 용량을 달성한다. 첫 번째 PUF 비트가 초기화 후의 안정 상태에서 발생하고, 이는 기존의 방식보다 4배 이상 안정적이다. 두 번째 비트는 동시에 추출된다. 이러한 접근 방식은 ECC를 완전히 제거하고 75-fJ/bit의 에너지 및 3.3%의 면적 오버헤드에서 SRAM의 작동 전압까지의 안정성을 향상시켜 표준 비트셀 재사용, 최소한의 면적 오버헤드, 127%의 PUF/SRAM 용량 비율 및 단 3.3%의 면적 오버헤드만으로 ECC-less 운영을 효과적으로 가능하게 한다.

#12-4 이 논문은 ultra-low-power 어플리케이션을 위한 새로운 dual-edge-triggered flip-flop (DET-FF)를 제시한다. Redundant internal node transition elimination (RTEDET)을 도입함으로써 동적 전력 소비를 최소화한다. DET-FF는 상승/하강 edge에서 데이터를 샘플링하여 클럭의 주파수를 절반으로 줄여 전력소모를 줄일 수 있다. 그러나 이 방식에서는 클럭의 내부 노드 전환이 중복으로 발생하는 문제가 있다. 이러한 불필요한 전환은 전력 낭비를 초래하는데, 이 논문에서 제안하는 RTEDET는 이러한 불필요한 내부 노드 전환을 제거한다. D (데이터)와 Q (출력)가 같을 때 클럭 버퍼는 이전의 값을 유지하여 불필요한 클럭 버퍼의 전환을 제거하여 전력 소비를 줄인다. 이러한 방식을 통해 최근 저전력 flip-flop와 비교하여 총 전력을 37~39% 줄였다. 또한, 이 RTEDET는 0.35V까지의 공급 전압에서 모든 칩에서 정적 작동 및 contention-free 기능으로 운영할 수 있다.

저자정보

박현준 박사과정 대학원생

- 소속 : 서울대학교
- 연구분야 : HBM, Chord Signaling, Information Theory
- 이메일 : spp098@snu.ac.kr
- 홈페이지 : https://sites.google.com/view/wschoi?pli=1