2024 International Solid-State Circuits Conference

(ISSCC) Review

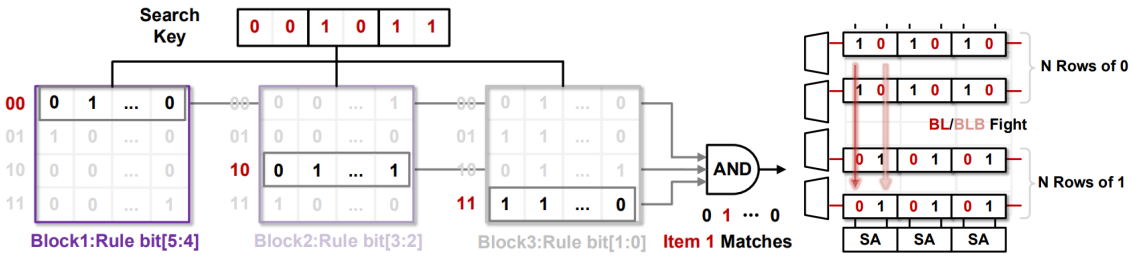
아주대학교 지능형반도체공학과 이종민 교수

Topic : Digital

Session 15 : Embedded Memories & Ising Computing

이번 ISSCC 2024의 Session 15는 Embedded Memories & Ising Computing이라는 주제로, 다양한 application에서 embedded memory의 성능을 높이는 점과, embedded memory를 활용한 논문들에 대해 주안점을 두고 있다. Technology의 scaling이 느려지고 있는 현 시점에서 칩의 성능을 높이기 위해서 embedded memory의 성능을 높이려는 논문들이 채택된 점을 주목할 만하다.

#15-1 은 Tsinghua University에서 발표한 논문으로, PUF를 기반으로 protect된 TCAM을 설계한 것이다. 기존 NOR-type과 NAND-type의 CAM cell은 많은 transistor를 필요로 하였으나, 본 논문에서는 6T 구조를 가져가 area efficiency를 향상시켰다. 또한, 기존의 TCAM의 병렬적인 비교 방식과는 달리, Search key를 2bit씩 나누고 해당 row의 mux를 켜, 6T SRAM cell로 인한 방전의 존재 유무로 데이터를 찾는다. 본 TCAM은 2N개의 선택된 row중 N개의 row에는 0을, 나머지 N개에는 1을 write하고, 이들을 하단의 sense amplifier로 비교하여 KEY를 생성한다. 생성된 KEY를 보안 인증에 활용하여 공격자가 security protocol을 bypass하거나, 데이터 패킷을 바꾸고 drop하는 것을 방지할 수 있다.

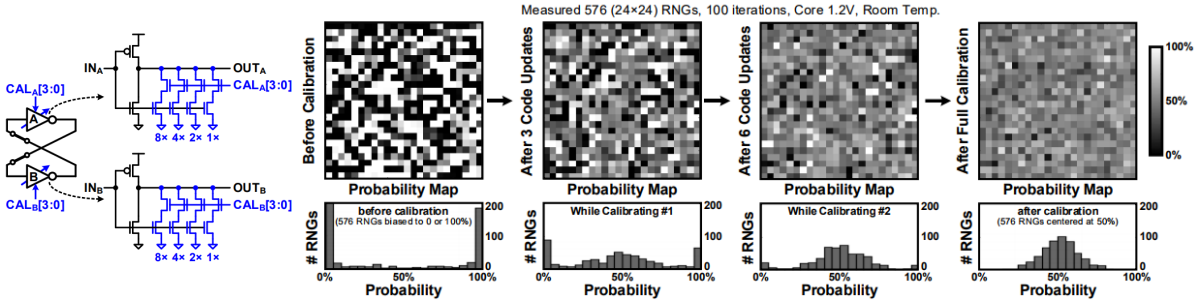


[그림 1] #15-1에서 (좌)제안한 TCAM의 search 방법 (우)PUF로의 활용

#15-2 는 Intel에서 발표한 논문으로, 기존에 frontside에서 전원 공급과 신호 전달을 했던 것과는 달리, 전원 공급을 위해 backside에 저항이 낮은 interconnect를 활용한 것에 대해 소개하고 있다. Backside에서 큰 PowerVia를 활용하여 SRAM bitcell에 전원을 직접 공급하면 SRAM 단위 셀 면적이 증가하는 단점이 있다. 따라서, SRAM array 외부에만 PowerVia를 사용하는 around-the-array power-delivery scheme을 활용하여, SRAM 단위 셀 면적 증가를 방지하였다. 이를 통해 기존보다

40mV 더 낮은 V_{min}과 14%의 performance 증가를 달성하였다.

#15-5 는 University of California, Santa Barbara에서 발표한 논문으로, Ising model 연산을 가속할 수 있는 Latch 기반의 Ising computer에 대한 논문이다. 23년도 ISSCC에서 발표한 Ising model 연산을 위한 latch에 calibration 구조를 추가하여 spin의 randomization을 수행 가능케 하여, RNG를 위한 면적 overhead를 제거하였다. 또한 replica끼리의 equalization을 통해 더 짧은 시간 내에 더 낮은 Hamiltonian에 도달할 수 있다.

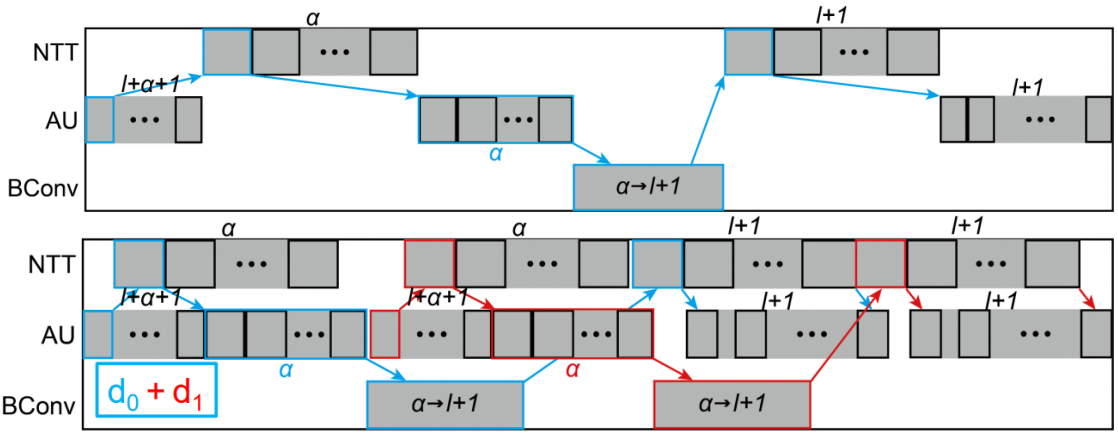


[그림 2] #15-5에서 제안한 calibration 구조가 추가된 latch와 이를 활용한 randomization 결과

Session 16 : Security: From Processors to Circuits

이번 ISSCC 2024의 Session 16은 Security: From Processors to Circuits 라는 주제로, 총 8편의 논문이 발표되었다. Homomorphic encryption accelerator, PQC processor, PUF, Side-channel attack resilient circuits, TRNG 등 hardware security에 필요한 Processor 부터 Circuit에 대해 소개하였다. 양자컴퓨팅 시대를 앞둔 만큼 PQC processor, homomorphic encryption 관련 논문들이 떠오르고 있는 점을 주목할 만하다.

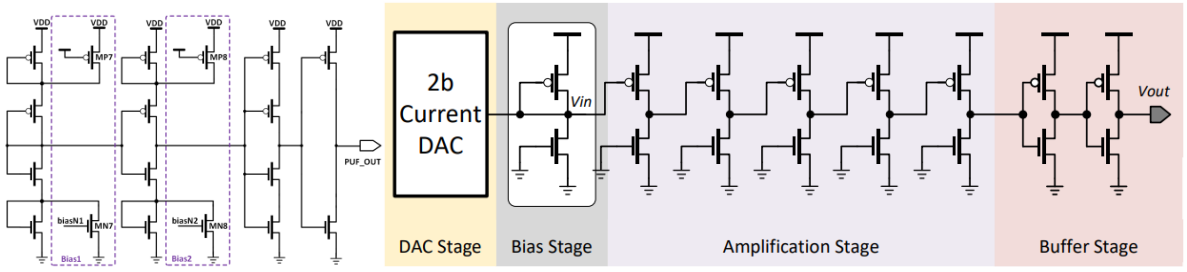
#16-1 은 포항공과대학교에서 발표한 논문으로, homomorphic encryption (HE) 알고리즘 중 하나인 RNS기반 CKKS를 위한 processor를 설계한 것이다. Cloud computing 시대의 도래로, 공격자가 cloud server를 공격하여 client의 데이터를 악의적으로 취득하는 것을 방지하기 위해, 암호화 된 상태에서 연산이 가능한 RNS-CKKS 알고리즘이 2018년에 제안되었고, 이를 전용 프로세서 구현을 통해 가속화 하였다. HE의 bootstrapping 연산에서 key-switch와 NTT/INTT 연산의 energy consumption이 크다는 점에 착안하여, key-switching 과정의 scheduling을 최적화하고 NTT 엔진의 twiddle factor generator를 통해 twiddle factor seed 사용을 99.9%가량 줄일 수 있었다. 이를 통해 CPU 대비 1737배의 key-switch energy efficiency 향상과, 25배의 throughput 향상을 달성할 수 있었다.



[그림 3] #16-1에서 제안한 (위) Conventional key-scheduling (아래) Optimized key-scheduling

#16-3 은 Marvell Technology에서 발표한 논문으로, PUF에 관해 발표한 것이다. 기존 PUF 대비 선단 공정인 3nm 공정에서 제작되었으며, entropy source간의 mismatch를 크게 증폭시키기 위하여 Gain NFET을 추가하였다. 이를 통해 V(BLT)-V(BLC) 값이 추가적으로 증폭되어 BER을 감소시킬 수 있다. 이를 통해 34.8ppm 수준의 낮은 BER을 달성하였다.

#16-4 는 NVIDIA에서 발표한 논문으로, University of Michigan과 Rice University에서 발표한 PUF를 개량하여, High-Density PUF와 Low-Power PUF 두 가지 PUF의 cell을 제안하였다. High-Density PUF는 단순히 inverter chain PUF cell의 첫 번째와 두 번째 stage에 diode connected TR과 bias injection TR을 추가하여 안정성 향상을 도모하였고, Low-Power PUF는 2T-AMP based PUF에 2b current DAC 기반 bias stage를 추가하였다. 5nm공정에서 설계되었으며, masking 한 것 대비 상당한 BER reduction을 달성하였다. 다만, prior work 대비 BER과 1bit response 생성 당 필요한 energy가 더 높다.

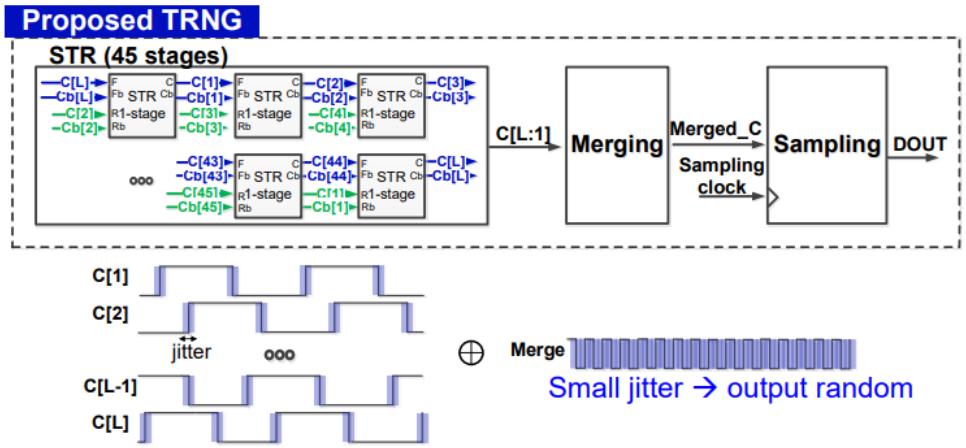


[그림 4] #16-4에서 제안한 (좌) High-Density cell (아래) Low-Power cell

#16-5 는 Rice University에서 발표한 fault injection attack (FIA) monitor에 대한 논문이다, 23년도 ISSCC에서 발표된 논문은 AES에 국한된 단점을 가지고 있고, 22년도 VLSI에서의 논문은 clock FIA만 detect하는 등의 단점들을 보완한 논문으로, clock의 replica를 만들고, replica의 falling edge 앞

뒤로 acceptance window를 구성하여, clock이 비정상적인 duty로 인해 window 외부에서 변화하거나, voltage glitch로 인해 window가 이동하는 경우 공격을 받았다고 간주한다. 본 논문에서 제안하는 FIA monitor 회로는 모두 디지털 회로로 설계되기 때문에, fully synthesizable하며, 굉장히 작은 면적을 소비하면서도 clock, voltage, EM, temperature FIA 모두를 cover한다.

#16-8 는 Samsung에서 발표한 TRNG에 대한 논문으로, 보안에 필요한 cryptographic KEY를 생성하기 위한 목적으로 만들었다. Entropy를 Self-Timed Ring (STR) 구조에서 취득하는 구조를 사용하였으며, STR cell의 각 stage에서 발생한 random jitter를 merge하여, random한 output을 생성하도록 설계하였다. 또한, 제안하는 TRNG 구조에서의 P(1), σ_{total}, σ_{total}^2, $cycle_{need}$ 등을 수학적 모델로 표현한 점이 돋보인다. 본 TRNG는 4nm 공정에서 설계되었으며, P(1), 8-bit chi-square, autocorrelation, min-entropy 및 10가지 type의 non-IID 측정 결과를 통해, TRNG가 가져야 할 여러 측정 결과들을 검증하였음을 확인할 수 있다.



[그림 5] #16-8에서 제안한 STR TRNG의 구조와 jitter 병합을 통한 난수 생성 방법

저자정보

이종민 교수

- 소　　속 : 아주대학교 지능형반도체공학과
- 연구분야 : Security Circuits, Low-power Digital Circuits
- 이 메 일 : jongmin@ajou.ac.kr
- 홈페이지 : https://sites.google.com/ajou.ac.kr/aisic