2025 International Solid-State Circuits Conference

(ISSCC) Review

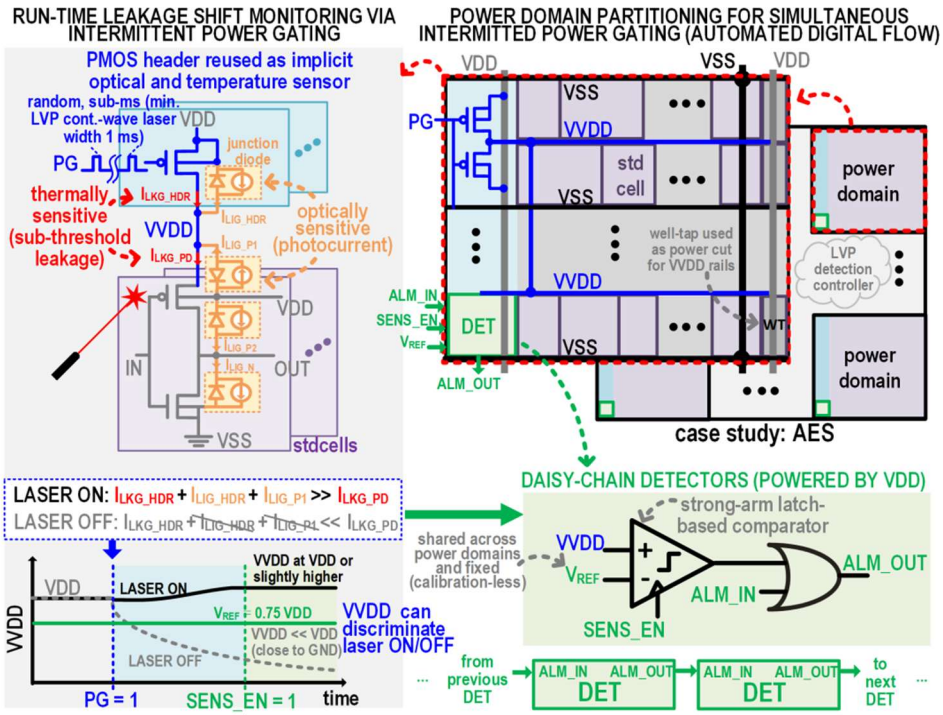
아주대학교 지능형반도체공학과 이종민 교수

Topic : Security

Session 17 : Hardware Security

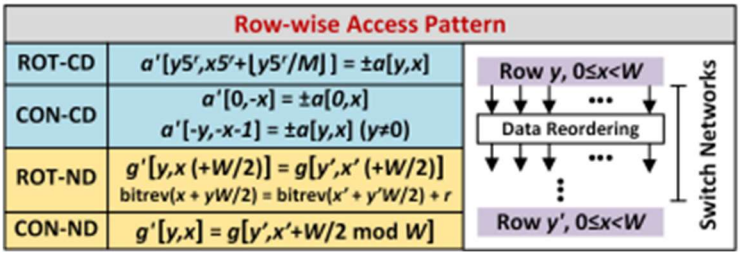
이번 ISSCC 2025의 Session 17은 Hardware Security라는 주제로, 동형 암호 가속에 대한 논문 2편, Physically Unclonable Function (PUF) 논문 2편, 그리고 Side-channel attack 방지 회로에 대한 논문 2편이 발표되었다. 특히, 작년에 이어 동형 암호 가속에 대한 논문이 발표되고 있는 점과, PUF의 새로운 안정화 방법에 대한 논문이 발표되고 있음을 주목할 만 하다.

#17-1 은 National University of Singapore에서 제안한 논문으로, LVP (Laser Voltage Probing) 공격을 탐지하는 회로를 제안하였다. 기존의 탐지 회로들은 PVT (Process, Voltage, Temperature)에 취약하거나, 면적 overhead가 큰 한계가 있었다. 그러나, 제안하는 연구에서는 추가적인 센서 없이 PMOS sleep transistor를 활용하여 LVP 공격을 감지하였다. 일정 영역별로 PMOS header, DET 구조를 배치하고, laser attack이 감지되는 경우 DET의 strong-arm latch에서 ALM 신호가 활성화 되도록 설계하였다. 넓은 영역의 LAP 공격을 감지하기 위해 ALM 신호를 DET끼리 연결하여 최종 ALM 신호를 생성하도록 하였다. 이를 통해 4.35%의 area overhead 만으로도 LAP 공격을 감지하는 구조를 설계하였다.



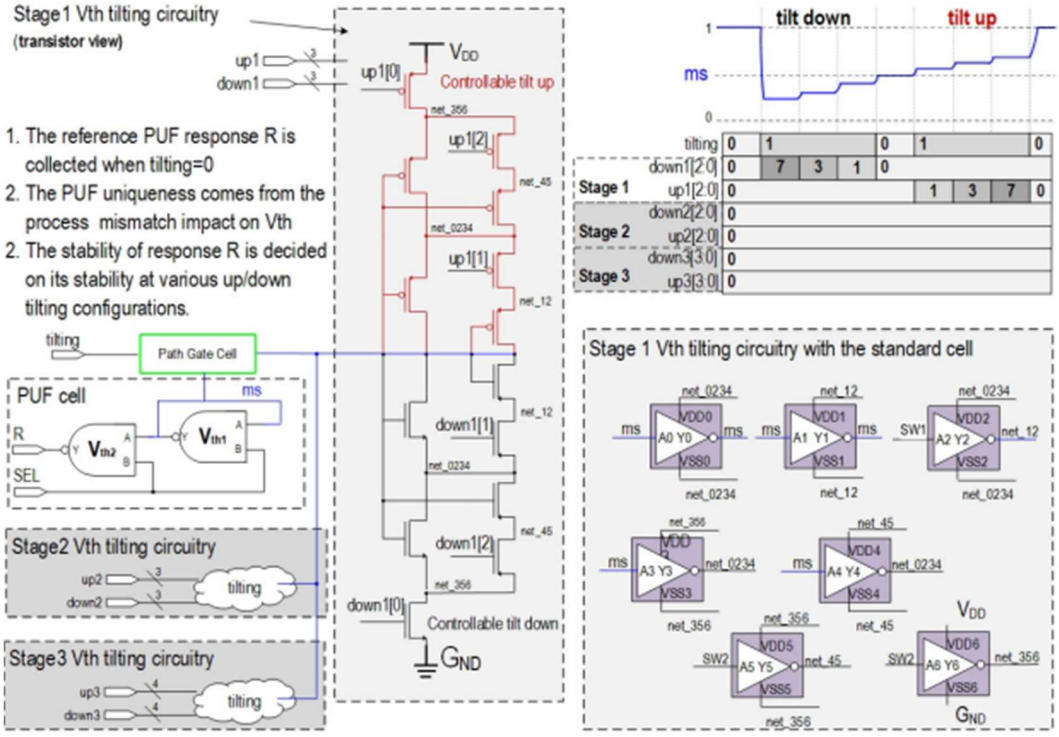
[그림 1] #17-1에서 제안한 LVP 공격 감지 회로 및 동작방법

#17-3 은 National Taiwan University에서 발표한 논문으로, multi-key CKKS 알고리즘 가속을 위한 프로세서를 제안하였다. 특히, NTT (Number Theoretic Transform)이 가장 많은 작업이므로, NTT를 기준으로 최적화하여 연산 속도를 향상시켰다. 또한, 불규칙한 데이터 접근 패턴을 가지는 ROT, CON 연산들에 대해 기존보다 빠르게 수행할 수 있도록 효율적인 dataflow를 설계하였다.



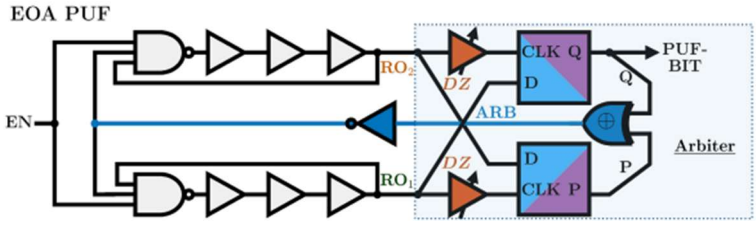
[그림 2] #17-3에서 제안한 ROT, CON 연산

#17-4 은 삼성전자 Foundry 사업부에서 발표한 논문으로, 2016년 및 2020년도 ISSCC에 발표한 PUF의 구조에 tilting 기법을 적용하였다. PUF의 cell 구조는 2016년도에 개발된 NAND gate를 직렬로 연결한 구조를 활용하고 있으며, 본 논문에서 주목할 점은 controllable tilting 구조를 제안하였다는 점이다. 특히, controllable tilting 회로는 standard inverter cell로 간단하게 구현할 수 있어, non-recurrent engineering cost를 낮출 수 있는 부분 중 하나이다. Tilting 회로는 NAND gate들 간의 mismatch가 작아 unstable한 response를 생성하는 cell들을 screening 하여 제거할 수 있다. 제안하는 구조는 8nm FinFET, 3nm GAA 공정에서 제작되었으며, 다양한 corner, temperature, supply voltage에 따라 reproducibility를 검증하였다. 또한, NIST SP 800-90b test를 통해 non-IID entropy estimation score도 검증하였다.

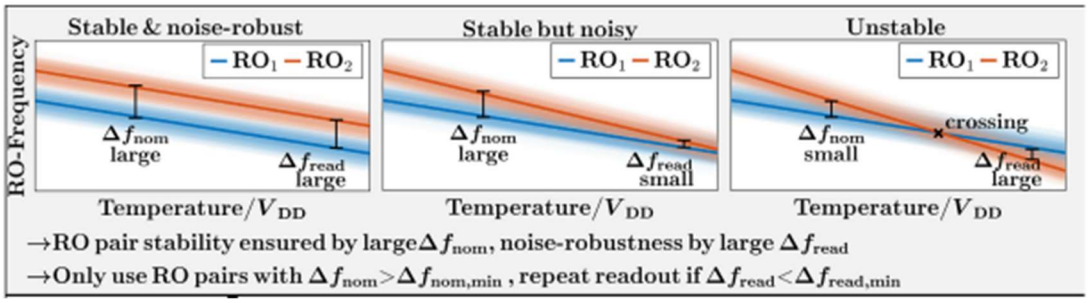


[그림 3] #17-4에서 제안한 controllable tilting 회로 및 제어 방법

#17-5 은 독일 University of Ulm에서 발표한 논문으로, [그림 4]와 같은 Arbiter PUF 구조를 활용하여 random response를 생성하였다. 본 논문의 장점으로는 자동화된 에러 감지 기능으로, response의 unstable한 state와 noisy한 state를 구분하여 분석하였다. [그림 5]의 좌측과 같이 안정적이고 noise robust한 cell들 만을 원하지만, 가운데 그림과 같이 noise에 취약하거나, 우측 그림과 같이 외부 환경 변화에 따라 response가 뒤집히는 현상이 발생한다. 이렇게 불안정한 response를 스스로 감지하기 위해, ARB신호를 생성하였고, ARB 신호가 0인 경우 readout을 반복하여 자동화된 에러 감지를 가능케 하였다.



[그림 4] #17-5에서 제안한 EOA PUF 구조



[그림 5] #17-5의 온도 및 supply voltage의 변화에 따른 RO의 frequency

#17-6 은 NVIDIA에서 발표한 논문으로, clock glitch 공격을 탐지하면서 안정적인 reference clock을 제공하는 RC oscillator를 제안하였다. [그림 6]의 제안하는 구조는 90°씩 shift된 4-phase의 clock을 sampling하여, glitch를 감지하였다. 또한 clock-glitch filter를 통해 $1/4F_{VCO}$ 보다 짧은 pulse를 filtering 하였다.

참고문헌

#17-1 H. Zhang, et al., "Sensor-Less Laser Voltage-Probing Attack Detection via Run-Time-Leakage-Shift Monitoring with 4.35% Area Overhead," *IEEE International Solid-State Circuits Conference (ISSCC)*, Feb. 2025.

#17-3 L-H. Lin, et al., "A 30.4GOPS/mW MK-CKKS Processor for Secure Multi-Party Computation," *IEEE International Solid-State Circuits Conference (ISSCC)*, Feb. 2025.

#17-4 B. Karpinskyy, et al., "An Efficient V_{th}-Tilting PUF Design in 3nm GAA and 8nm FinFET Technologies," *IEEE International Solid-State Circuits Conference (ISSCC)*, Feb. 2025.

#17-5 B. Driemeyer, et al., "An Eye-Opening Arbiter PUF for Fingerprint Generation Using Auto-Error Detection for PVT-Robust Masking and Bit Stabilization Achieving a BER of 2e-8 in 28nm CMOS," *IEEE International Solid-State Circuits Conference (ISSCC)*, Feb. 2025.

#17-6 N. Metha, et al., "A 100MHz Self-Calibrating RC Oscillator Capable of Clock-Glitch Detection for Hardware Security in a 3nm FinFET Process," *IEEE International Solid-State Circuits Conference (ISSCC)*, Feb. 2025.

저자정보

이종민 교수

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