2025 IEEE VLSI Review

한국과학기술원 석사과정 윤지원

Session 16 Hardware Security

이번 2025 IEEE VLSI의 Session 16은 Hardware Security라는 주제로 총 4편의 논문이 발표되었다. 이는 반도체 칩과 시스템 설계 단계에서 발생할 수 있는 보안 위협에 대응하기 위한 회로 아키텍처 수준의 기술들을 다루는 분야이며, 이 섹션은 칩 설계와 보안을 융합한 연구를 통해 신뢰성있고 안전한 하드웨어 구현을 목표로 했다.

#16-2 본 논문에서는 보정(calibration) 과정 없이도 안정적으로 동작하는 래치 기반 TRNG (Tolerant Latch-Based True Random Number Generator) 를 제안한다. 제안된 회로는 두 인버터와 두 커패시터로 이루어진 직렬 커패시터 연결 cross-coupled latch 구조를 활용하여 auto-zero 단계에서 불일치를 체계적으로 상쇄하고, 이후 잡음만을 증폭함으로써 출력 결정이 본질적인 잡음에 의존하도록 설계되었다. 특히 기존 shunt 방식의 auto zeroing 에서 발생하는 기생 커패시턴스에 대한 offset 샘플링 오류를 근본적으로 제거하는 series-based auto zeroing 기법을 도입하여, 보정 회로 없이도 높은 난수 품질을 확보하였다. 또한 네 개의 셀을 병렬로 결합하여 편향 확률을 효과적으로 줄이고, 설계 복잡도를 완화함으로써, 초미세 공정 환경에서도 소형 저전력 동작과 함께 높은 보안 강도와 실용성을 동시에 달성하였다.

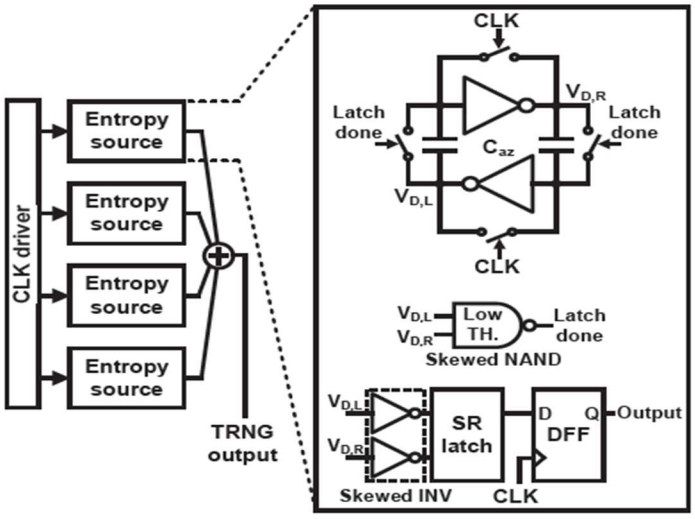
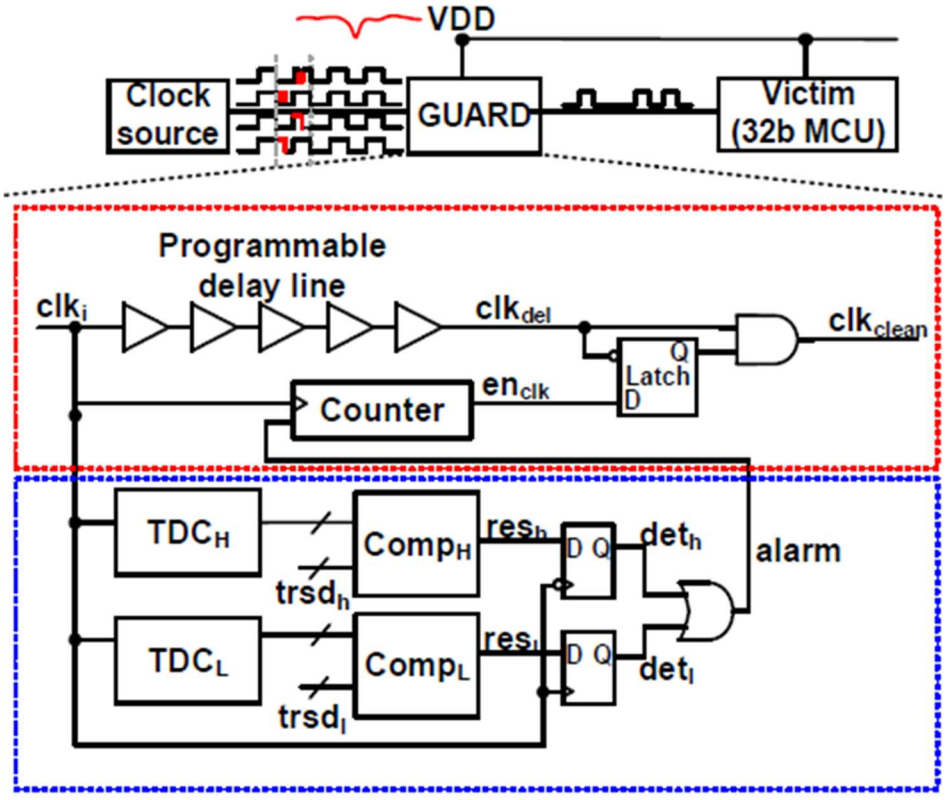


Fig. 2. Proposed TRNG system with multiple entropy sources

[그림 1] 다중 엔트로피 소스를 이용한 제안된 TRNG 시스템

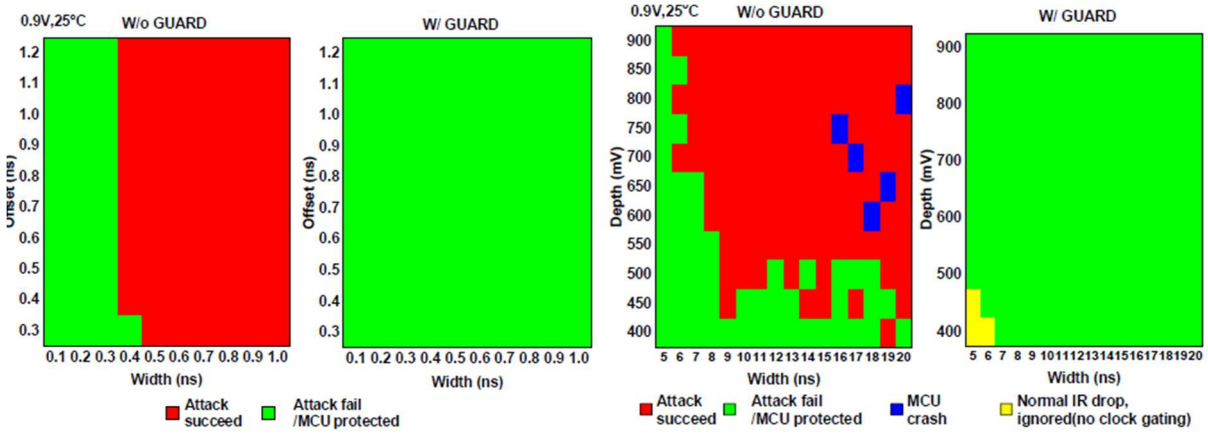
실험 결과, 제안된 TRNG는 4nm FinFET 공정에서 제작되어 PVT 코너와 공급 전압, 온도 변동, 그리고 최대 200mV의 전원 노이즈가 주입된 조건에서도 안정적으로 동작하였다. 0.75V에서 1.7pJ/bit의 우수한 에너지 효율을 달성했으며, 최소 엔트로피는 전 주파수 범위에서 0.99 이상을 유지하였다. 또한 NIST SP 800-22와 SP 800-90B 검증에서 각각 97.9% 이상의 통과율과 안정적인 엔트로피 특성을 보여, 추가적인 보정 없이도 최신 설계 대비 동등하거나 더 우수한 난수 품질을 입증하였다. 이를 통해 제안된 TRNG는 초소형, 저전력 환경에서도 높은 신뢰성과 보안성을 제공할 수 있음을 확인하였다.

#16-3 본 논문은 클록 및 전압 글리치를 이용한 오류 주입 공격이 하드웨어 보안에 심각한 위협이 됨을 지적하며, 기존 DLL, FLL 기반 탐지 회로들이 보호 기능의 부재, 정상 전원 노이즈와의 구분 불가, 실제 공격 검증 부족, 높은 내부 클록 요구 등 한계를 지닌다고 설명한다. 이에 대응하여 저자들은 GUARD 라는 새로운 탐지기를 제안하는데, 이는 최적화된 TDC (Time-to-Digital Converter) 를 이용해 클록 펄스 이상을 감지하고, 전압 글리치로 인한 지연 변화를 탐지하며, 탐지 즉시 클록 게이팅을 통해 피해 프로세서의 오류 발생을 방지하는 on-demand 보호 기능을 제공한다. GUARD는 공정, 전압, 온도 변동에도 강인하며 단일 및 다중 글리치 공격을 모두 차단할 수 있는 실용적인 하드웨어 보안 솔루션임을 강조한다.



[그림 2] GUARD의 블록 다이어그램 (하단의 파란색은 탐지기, 상단의 빨간색은 보호기로 구분됨)

본 논문에서 제안하는 GUARD 는 탐지기와 보호기로 구성된 구조로, 탐지기는 두 개의 TDC 와 비교 모듈을 통해 클록의 high/low 펄스 폭을 모니터링하여 이상 시 알람을 발생시키고, 보호기는 클록 지연선, ICG, 카운터를 활용해 공격이 탐지되면 즉시 클록을 게이팅하고 안정적인 신호가 회복될 때까지 대기함으로써 피해 MCU 의 오류 발생을 차단한다. 특히 TDC 회로를 최적화하여 100ps 간격의 빠른 펄스도 감지 가능하며, 탐지 직후 내부 노드를 빠르게 초기화해 즉시 재사용할 수 있도록 설계되었고, 비트 수준 산술 회로를 적용해 임계 경로 지연을 절반으로 줄여 고주파 클록 환경을 지원한다. 또한 테스트 칩에 32bit RISC MCU 와 on-chip 글리치 발생기를 포함해 실제 공격 시나리오를 재현, 특정 명령어를 건너뛰어 보안 검사를 회피하는 공격 모델에서도 효과적으로 대응함을 입증하였다.

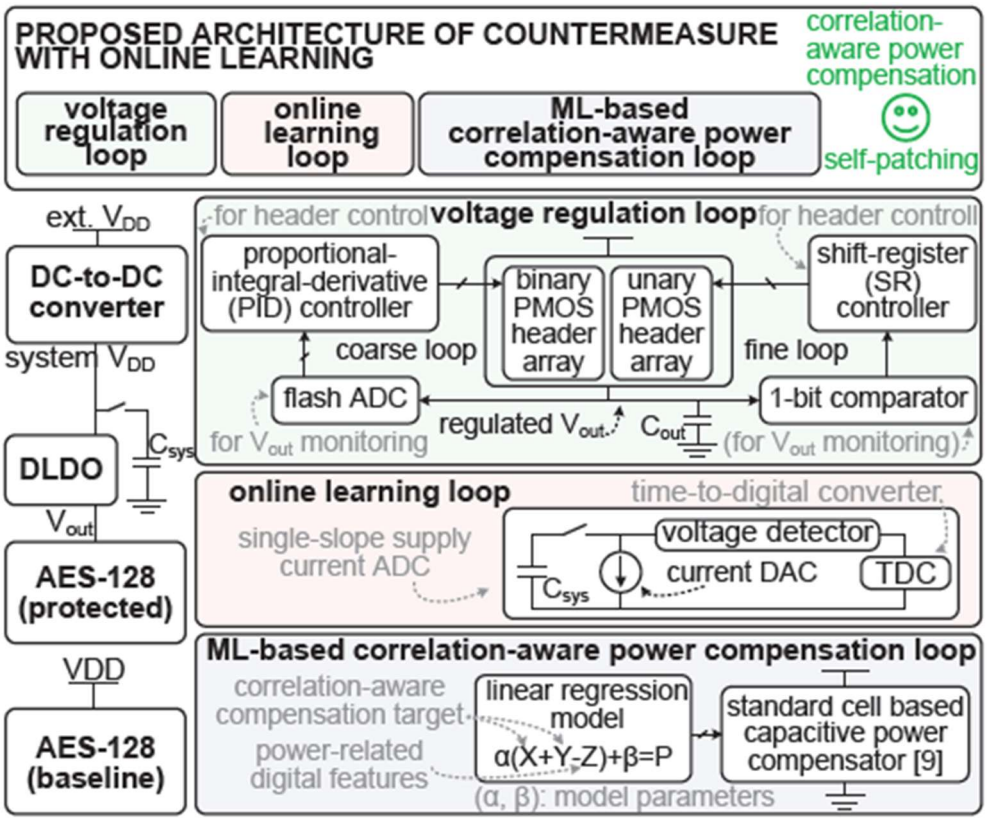


[그림 3] GUARD의 보호 성능 측정 결과: (왼쪽) Clock glitch 공격, (오른쪽) Voltage glitch 공격

Measurement 결과, 28nm CMOS 로 제작된 GUARD 테스트 칩은 실제 글리치 공격 실험에서 클록 및 전압 글리치 모두에 대해 100% 방어 성공률을 달성하였으며, 정상적인 동적 IR drop 과 공격을 구분하여 불필요한 보호 동작을 방지할 수 있음을 입증하였다. 또한 -40~125 ℃의 넓은 온도 범위에서도 안정적으로 동작하였고, 기존 연구들과 비교해 최초로 탐지와 보호를 동시에 제공하며, 희생 프로세서를 포함한 실제 공격 실험을 통해 그 효과성을 검증한 점에서 차별성을 가진다.

#16-4 본 논문은 전력 분석 사이드 채널 공격 (SCA)에 대응하기 위한 새로운 접근으로, on-chip online 학습 기반 대응책을 최초로 제안한다. 기존의 WDDL, 마스킹, 비동기 회로, 레귤레이터 기반 기법 등은 공정 편차로 인한 칩별 특성과 시간에 따른 노화 현상에 적응하지 못해 보안성이 점차 저하되는 한계를 지닌다. 저자들은 이를 해결하기 위해 칩 내부에서 전력 파형을 디지털화하고, 이를 기반으로 전력 보상 머신 러닝 모델을 지속적

으로 학습시켜 mismatch 와 aging 효과를 보장하는 자율 보안 관리 방식을 구현하였다. AES-128 코어 실험을 통해 이 방법이 노화로 인한 18,000배 보안 열화를 완전히 상쇄하고, 최신 최고 수준의 공격 내성(MTD)을 달성함을 입증하여, 장기적으로 안정적이고 칩 맞춤형 보안을 제공할 수 있음을 보여준다.

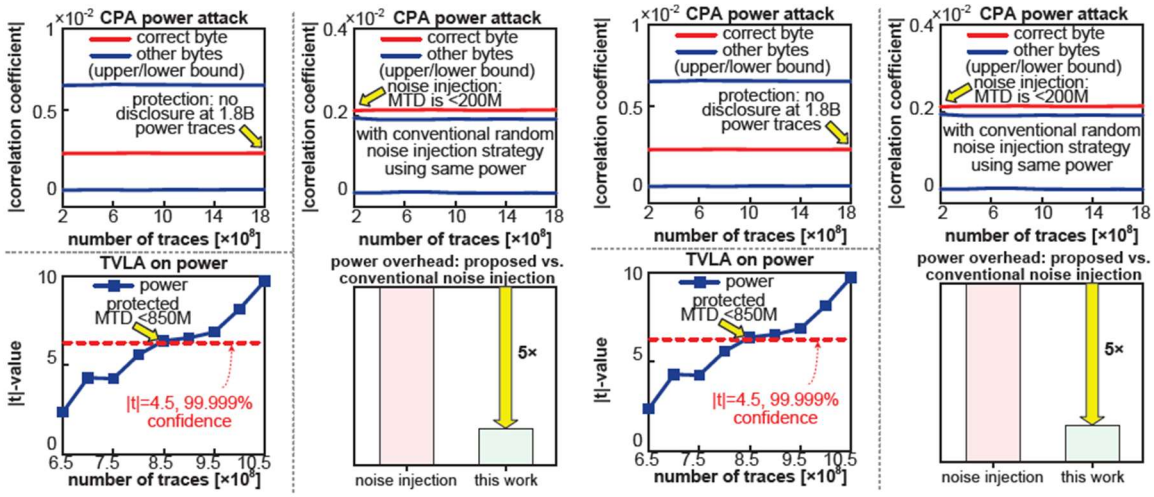


[그림 4] 전력 분석 공격에 대한 제안된 온라인 학습 기반 대응 기법: 디지털 LDO 기반 전력 디지털화 및 ML기반 전력 보상

이 논문은 AES 코어를 보호하기 위해 전류 측정-온라인 학습-전력 보상으로 이어지는 아키텍처를 제안한다. 전력 공급은 DC-DC와 DLDO 기반 루프가 담당하며, AES 전류는 단일 슬로프 current ADC와 TDC를 통해 디지털화된다. 이후 온라인 학습 루프가 활성화되면, 정보 민감 사이클에서 AES를 Csys로부터 구동하고 방전 시간을 측정해 평균 전류를 얻은 뒤, 이를 선형 회귀 기반 ML 모델에 학습시켜 칩별 불일치와 PVT 변동, aging 효과를 보정한다. 학습된 가중치는 전력 보상 루프에 적용되어 AES 연산 feature와 실제 전력 간 상관관계를 무작위화하는 에너지 마스킹으로 이어지며, 이를 통해 추가 회로 부담 없이 장기간 안정적이고 칩 맞춤형 보안을 달성한다.

실험 결과, 제안된 온라인 학습 기반 대응책은 40nm AES 테스트 칩에서 MTD 18만배, TLVA 106만배 향상으로 최고 18억 트레이스 수준의 공격 내성을 달성하였으며, 기존 노이즈 주입 대비 전력 오버헤드는 5배 낮았다. 또한 가속 노화 실험에서 온라인 학습이 없으면 MTD가 10만으로 급락했지만, on-chip 학습을 통해 단 한 번의 학습만으로도 보안성이 완전히 회복되었고, 반복 재학습이 필요 없었다. 더 나아가 모델 학습 속도가 공격자의 off-chip 학습 보다 훨씬 빨라, 1초 미만

의 사전 학습으로도 장기적이고 칩 맞춤형 보안을 제공할 수 있음을 입증하였다.



[그림 5] 보호되지 않은 AES (왼쪽) 과 제안된 on-line 학습 기반 보호 AES (오른쪽) 의 전력 분석 공격 내성 비교

저자정보

윤지원 석사과정 대학원생

- 소속 : 한국과학기술원 (KAIST)
- 연구분야 : 디지털 회로 설계
- 이메일 : jwyoon@ics.kaist.ac.kr
- 홈페이지 : https://ics.kaist.ac.kr