

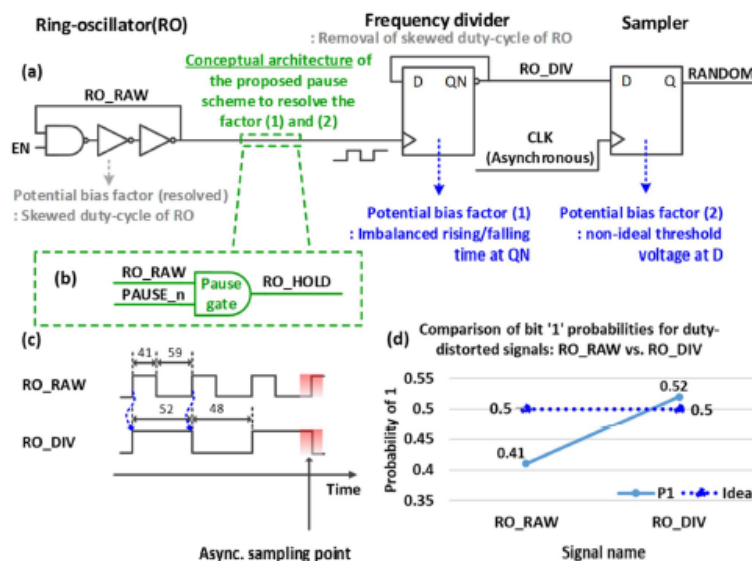
2026 VLSI Review

한국과학기술원 전기및전자공학부 석사과정 박성용

Session 12 True Random Number Generators

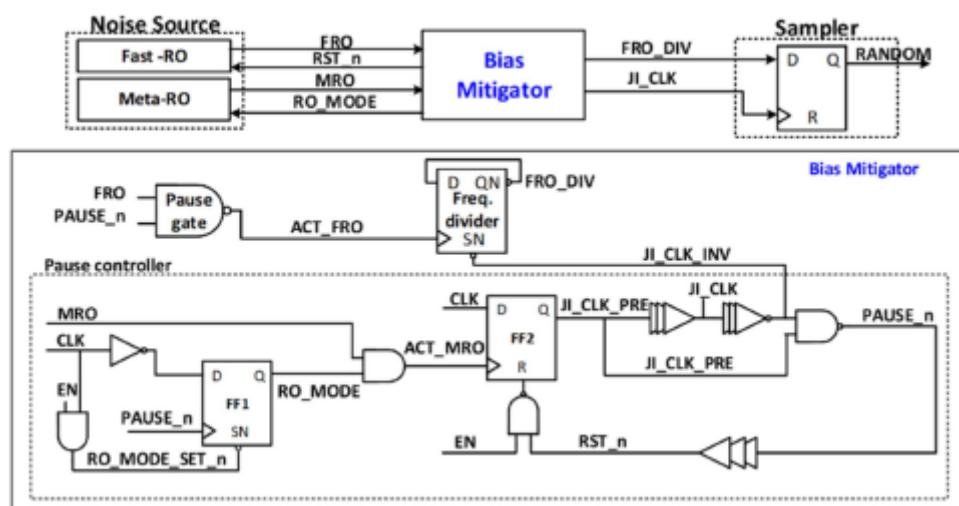
이번 Session 12에서는 총 4편의 TRNG(True Random Number Generator) 관련 논문이 발표되었다. TRNG는 반도체 회로에서 발생하는 물리적 noise를 이용해 0 또는 1의 랜덤 비트를 생성하는 회로이다. 아래의 논문들은 각각 advanced-node에서 기존 RO(Ring Oscillator) 기반 TRNG의 bias를 직접 제거하는 방법과, differential CMOS thyristor를 이용하여 후처리 없이 높은 엔트로피를 얻는 방법을 통해 TRNG 하드웨어의 문제를 해결하는 데에 중점을 두었다.

#12-1 삼성전자의 논문은 4nm FinFET 공정에서 RO 기반 TRNG의 bias를 줄이면서 기존 RO 구조의 단순성과 작은 면적을 유지하고자 하였다. RO 기반 TRNG는 oscillator의 phase jitter를 비동기적으로 샘플링하여 랜덤 비트를 생성하므로 구조가 단순하지만, RO의 duty-cycle이 50%에서 벗어나면 0과 1의 샘플링 확률이 달라진다. 이를 보정하기 위해 frequency divider를 사용하더라도 선단 공정에서는 divider의 상승 및 하강 트랜지션 시간 차이와 샘플러 D 입력의 비이상적 threshold가 새로운 bias 원인이 될 수 있다. 본 연구는 이러한 bias가 RO 자체뿐 아니라 랜덤 비트를 받아들이는 플립플롭과 샘플러에서도 추가로 발생한다는 점에 주목하고, 샘플링 직전에 RO 트랜지션을 일시적으로 차단하는 Bias Mitigator를 제안하였다.



[그림 1] 기존 RO 기반 TRNG의 bias 원인과 pause-gate 기반 bias mitigation

그림 1은 기존 RO 기반 TRNG에서 bias가 발생하는 원인과 제안된 회로의 기본 아이디어를 보여준다. 일반적인 구조에서는 frequency divider를 사용하면 RO의 duty-cycle 불균형을 줄일 수 있다. 선단 공정에서는 divider 내부의 상승·하강 전이 특성이나 샘플러의 비이상적인 입력 threshold로 인해 0과 1이 유지되는 시간이 달라질 수 있다. 이 경우 비동기적으로 샘플링되는 0과 1의 확률이 달라져, TRNG 출력 비트가 1일 확률인 $P(1)$ 이 이상적인 값인 0.5에서 벗어나게 된다. 제안된 구조는 divider 앞에 pause gate를 추가하여, 샘플링 직전에 새로운 트랜지션을 차단함으로써, 플립플롭의 트랜지션 불균형과 샘플러 threshold가 샘플링 결과에 미치는 영향을 줄일 수 있다. 이를 통해 복잡한 calibration 없이, 현재 값이 0인지 1인지에 관계없이 동일한 조건에서 샘플링되도록 하여 divider와 샘플러의 비대칭이 최종 랜덤 비트의 bias로 이어지는 것을 억제한다.



[그림 2] Bias Mitigator가 포함된 dual-RO TRNG의 전체 구조

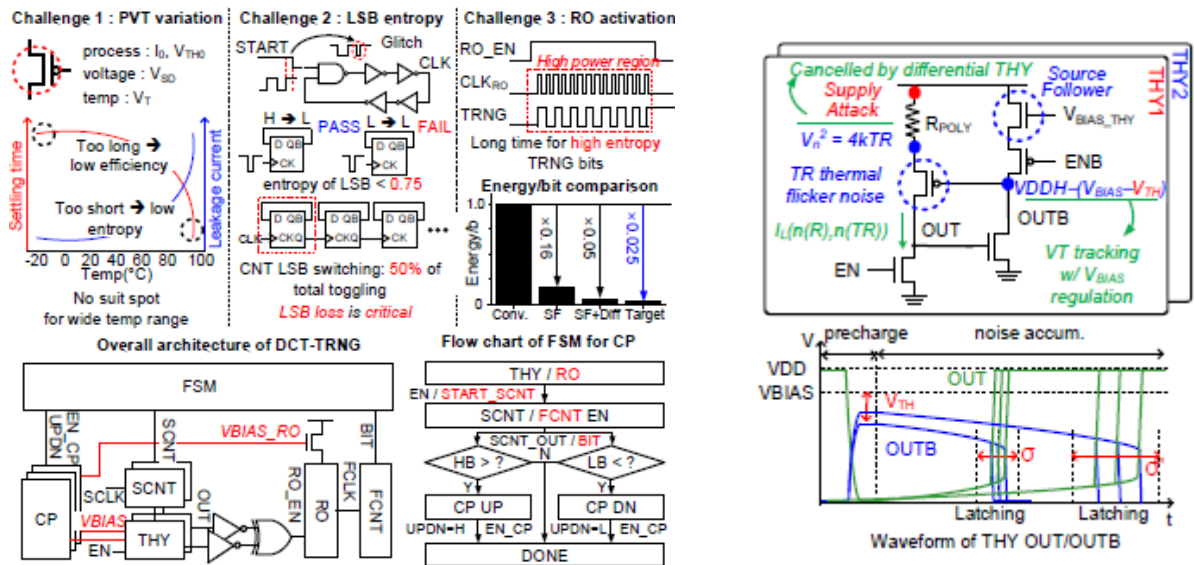
그림 2는 제안된 TRNG의 전체 구조이다. Noise source는 Fast-RO와 Meta-RO 두 경로로 구성된다. Meta-RO에서는 metastability에 의한 초기 위상 jitter와 이후 RO의 jitter를 함께 이용한다. Fast-RO는 독립적으로 jitter를 누적하며, frequency divider를 거친 FRO_DIV가 최종 샘플링 신호가 된다. Bias Mitigator는 pause gate, frequency divider, pause controller로 구성되며, Meta-RO의 첫 상승 엣지를 이용해 샘플링보다 먼저 PAUSE_n을 생성한다. 따라서 샘플링 직전의 변화를 정지시키고, Meta-RO의 무작위성 timing을 이용해 샘플러를 동작시킨다. 랜덤 비트 생성 이후 내부 상태를 리셋하여 이전 비트의 상관관계도 줄인다. 이를 통해 기존 dual-RO 구조의 jitter 기반 엔트로피 생성 방식은 유지하면서, divider와 샘플러의 mismatch에서 추가적으로 발생하는 bias를 억제하였다.

기존 RO 기반 TRNG에서는 RO에서 충분한 jitter를 생성하는 것뿐만 아니라, 생성된 무작위성을 최종 디지털 비트로 변환하는 샘플링 과정 또한 중요하다. 특히 선단 공정에

서는 소자의 mismatch가 증가하면서 frequency divider와 샘플러와 같은 회로의 작은 비대칭도 반복적인 샘플링 과정에서 bias로 이어질 수 있다. 이러한 문제를 별도의 복잡한 보정 회로나 후처리로 해결하는 대신, 샘플링 직전에 신호의 변화를 일시적으로 정지시키는 간단한 회로를 추가하였다.

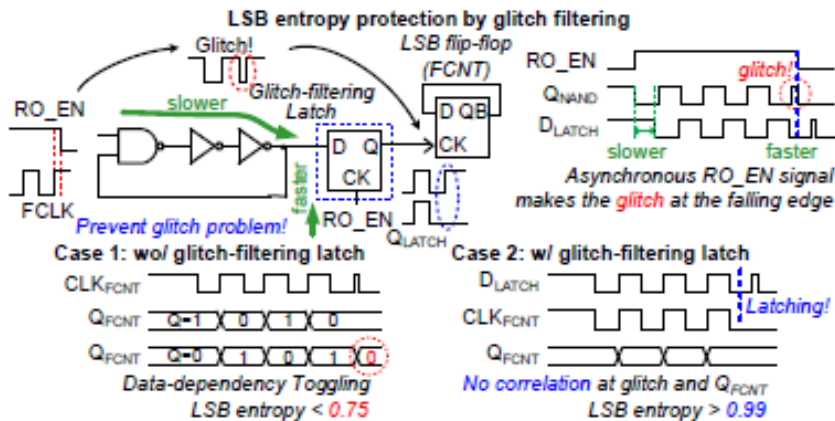
제안된 기법은 5개의 process corner에서 총 290개의 칩을 대상으로 0.675~0.935V, -40~150°C 범위에서 측정되었다. 대표 조건에서 Bias Mitigator를 사용하지 않은 P(1)은 0.4471이었으나 제안된 pause 동작을 적용하면 0.5013으로 개선되어 97.54%의 bias reduction을 보였다. NIST SP 800-90B 평가에서는 별도의 15개 칩을 사용하였으며 IID track에서 평균 0.986 bit/bit의 최소 엔트로피를 얻었다. 스루풋은 4Mbps, TRNG core 면적은 80.198 μm^2 , 소비전력은 2.16mW이다. 따라서 해당 연구는 미세공정에서 커지는 mismatch로 인한 bias를 간단한 샘플링 제어 회로로 억제하여 bias 개선 효과와 높은 최소 엔트로피를 확보하였으며, 이를 80.198 μm^2 의 작은 RO 기반 구조로 구현하여 선단 공정에서의 실용적인 TRNG 구현 가능성을 보여주었다.

#12-2 성균관대학교의 논문은 differential CMOS thyristor의 latching-time jitter을 엔트로피 소스로 사용하여 PVT 변화에 강하면서도 낮은 비트당 에너지를 갖는 후처리 없는 TRNG를 구현하고자 하였다. 기존의 시간 기반 TRNG는 noise를 충분히 누적하기 위해 RO를 오랫동안 동작시켜 에너지 소비가 크고, metastability 기반 TRNG는 mismatch와 PVT 변화에 민감하여 calibration이나 XOR 후처리를 사용하는 경우가 많다. 특히 XOR 방식은 일부 엔트로피 소스가 fault나 attack으로 deterministic하게 변하더라도 최종 출력이 랜덤하게 보일 수 있어 source failure가 가려질 수 있다. 이를 해결하기 위해 1) thyristor의 noise 누적 시간을 일정하게 유지하는 Bias Self-Regulation, 2) 비동기 RO disable에서 발생하는 glitch를 제거하는 Glitch-Filtering Latch, 3) 두 thyristor의 latching time 차이 동안에만 RO를 활성화하는 Differential Short-Window Activation을 포함한 DCT-TRNG 구조를 제안하였다.



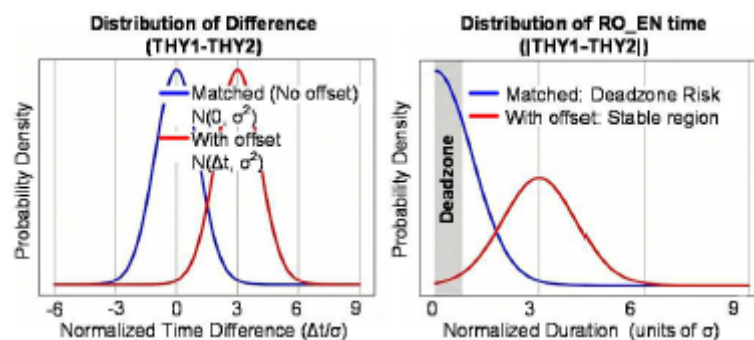
[그림 3] DCT-TRNG의 전체 구조와 CMOS thyristor의 noise 누적 원리

그림 3은 DCT-TRNG의 전체 구조와 엔트로피 소스의 동작을 보여준다. Thyristor는 누설전류에 의해 내부 노드가 천천히 변화하다가 피드백 조건에 도달하면 상태가 뒤집히며 latch되는 구조를 이용해 무작위성을 만들며, precharge부터 latching까지의 시간을 T_{acc} 로 정의한다. T_{acc} 에는 누설전류와 noise에 의한 jitter가 함께 포함되므로 시간 자체가 무작위성을 띤다. 그러나 누설전류는 PVT에 민감하여 고정된 bias에서는 저온에서 T_{acc} 가 너무 길어 에너지를 낭비하고, 고온에서는 너무 짧아 noise 누적이 부족할 수 있다. 이를 해결하기 위해 소스 팔로워로 PMOS를 weak inversion 영역에서 동작시키고, 시스템 클럭 카운터(SCNT)가 실제 T_{acc} 를 측정하여 FSM과 charge pump가 bias 전압을 조절한다. 동시에 주파수 카운터(FCNT)는 RO 주파수를 측정하여 time-to-digital 변환의 양자화 단계도 PVT에 따라 변하지 않도록 한다. Differential thyristor의 common source에 삽입된 폴리실리콘 저항은 common-mode supply noise를 줄이면서 differential noise 성분을 이용하도록 한다.



[그림 4] Glitch-filtering latch를 이용한 LSB entropy protection

카운터의 LSB는 가장 빈번하게 변화하는 비트이므로, LSB의 엔트로피가 낮아 이를 버리게 되면 비트당 에너지 효율이 크게 저하될 수 있다. 그림 4는 비동기 RO 활성 신호에서 발생하는 glitch가 LSB의 엔트로피를 낮추는 원인과 이를 해결하는 구조를 보여준다. 두 thyristor의 latching event로 만들어진 RO_EN은 시스템 클럭과 비동기이므로 하강 엣지가 카운터 클럭과 가까우면 짧은 glitch가 발생할 수 있다. 이 glitch가 카운터의 LSB 플립플롭에 직접 전달되면 이전 Q state에 따라 setup/hold violation의 결과가 달라져 데이터 의존 bias가 생기며, 논문에서는 LSB 최소 엔트로피가 0.75 이하로 감소할 수 있음을 보였다. 제안된 구조는 RO_EN 경로에 transparent latch를 삽입하여 glitch와 현재 Q state 사이의 상관관계를 제거한다. 이를 통해 LSB 최소 엔트로피를 0.99 이상으로 회복하여 가장 많이 toggle하는 LSB를 버리지 않고 사용할 수 있다.



[그림 5] Differential latching-time의 entropy deadzone

한편, 두 thyristor의 latching time을 최대한 같게 만드는 것이 항상 유리한 것은 아니다. 본 구조에서는 THY1과 THY2가 latch되는 시간 차이 동안만 RO가 활성화되므로 두 시간이 지나치게 가까우면 RO 활성 시간이 거의 0이 된다. 이 경우 $|THY1-THY2|$ 의 분포가 0에서 folding되면서 부호 정보를 잃고, RO가 충분한 엣지를 만들기 전에 비활성되어 zero-count가 반복될 수 있다. 저자들은 이를 엔트로피 데드존(entropy deadzone)으로 정의하였으며, RO 활성 시간이 약 9 ns 이하인 영역에서 NIST Runs test의 성공률이 급격히 저하됨을 확인하였다. 이를 해결하기 위해 두 thyristor의 평균 latching time에 약 45ns의 오프셋을 두었다. 이 오프셋은 무작위성을 만드는 값이 아니라 분포를 데드존 밖으로 이동시키는 역할이며, 사이클 간 편차는 여전히 누적된 noise에 의해 결정된다. 따라서 두 경로를 완전히 매칭하는 대신 최소 RO 활성 시간을 보장하여 엔트로피와 효율성 사이의 trade-off를 해결하였다.

28nm CMOS 공정에서 제작된 DCT-TRNG는 0.8V에서 13.3Mb/s의 스루풋과 0.33pJ/bit의 에너지 효율을 달성하였다. 5개 칩에 대해 0.8~1.1V, -40~125°C에서 측정된 새넨 엔트로피는 0.99999 이상으로 유지되었으며, NIST SP 800-22/90B test와 power-supply injection 조건에서도 raw random bit을 검증하였다. 제안된 구조는 XOR 후처리 없이 Bias Self-Regulation으로 PVT에 따른 noise 누적 시간을 유지하고, Glitch-Filtering

Latch로 LSB 엔트로피 손실을 막으며, 두 thyristor 사이에 오프셋을 두어 엔트로피 데드존에서 벗어났다. 따라서 엔트로피가 생성되어 디지털 비트로 변환되는 전체 경로의 실패 원인을 회로적으로 제거하여 낮은 비트당 에너지와 높은 엔트로피를 동시에 달성하였다.

저자정보



박성용 석사과정 대학원생

- 소속 : 한국과학기술원 전기및전자공학부
- 연구분야 : Digital Circuit Design, ECC Hardware Design
- 이메일 : sypark@ics.kaist.ac.kr
- 홈페이지 : <https://ics.kaist.ac.kr/>