# 모트 전이 소재 기반 초고속, 저전력, 변이 내성 진성 난수 발생기 개발

## Fast, low-power, and variation tolerant true random number generator based on a mott memristor

연구책임자 김경민 | 소속학과 신소재공학과 | 홈페이지 http://semi.kaist.ac.kr

난수 발생기 (Random Number Generator, RNG)란 정보의 암호화 과정에 필수적으로 이용되는 키 (key)를 생성하는 장치이다. 진성 난수 발생기(True Random Number Generator, TRNG)는 물리적인 무작위 현상을 기반으로 완전한 난수를 발생하는 장치로 차세대 보안 소자의 핵심 기술이다. 기존의 진성 난수 발생기는 무작위한 물리적 현상을 연산장치에서 이용할 수 있도록 디지털화하는 과정이 비효율적이고 느린 한계가 있었다. 본 연구에서는 열에 의해 저항 상태가 바뀌는 모트 전이 현상에서 열적 변동의 무작위성을 기반하여 진성 난수 발생기로 이용하는 방법을 최초로 제시하였다. 모트 전이 현상은 초고속, 저전력으로 동작이 가능하며, 멤리스터 기반의 TRNG 기술 중 가장 빠른 40 kb/s의 속도로 진성 난수 발생에 성공했다. 또한, 이 기술에서 이용하는 열적 변동은 주변 환경의 영향을 받지 않아 극한의 환경을 포함한 다양한 환경에서 활용할 수 있다.

## 1. 연구배경

보안 시스템은 제3자가 알 수 없는 암호를 활용하며, 이를 위해서는 하드웨어 기반의 진성 난수 발생기 (True Random Number Generator)가 필요하다. 기존 기술에서는 주로 CMOS (Complementary metal-oxide-semiconductor) 하드웨어 기반의 보안 기술이 사용되었는데, 이 경우 보안성이 낮고, 에너지 소모가 크고, 소자의 소형화가 어려운 한계가 있어 초연결 시대에서 하드웨어 보안 기술로 사용되기에 적합하지 않다. CMOS 기반 기술의 한계를 극복하기 위해 최근 TaOx, HfOx와 같은 산화물 저항 변화 소재의 저항 변화 과정에서의 본질적인 혼돈성 (Intrinsic stochasticity)을 이용한 하드웨어 기반 보안 기술이 연구되고 있다. 그러나 산화물 소재 기반의 하드웨어 기반 보안 기술은 많은 주변 회로를 요구하므로 집적화에 한계가 있음을 CMOS 기반 기술과 공유하며, 느린 난수 발생 속도로 인해 실제로 활용되기에 어려움이 있다. 따라서, 저면적에서 에너지 효율적으로 고속으로 구동 가능한 진성 난수 발생기 개발이 필요하다.

## 2. 연구내용

기존 진성 난수 발생기 기술은 무작위성의 원천으로 확산형 멤리스터나 전하 트랩형 멤리스터를 이용하였으나, 이온 확산 및 전하 트랩 현상은 수 마이크로초(us) 규모의 시간에서 느리게 일어나므로 난수 발생 속도에 제한이 있다. 모트 전이 (Mott-transition)는 절연체-금속 전이 (Insulator-Metal Transition)로써 특정 온도에서 소재가 부도체에서 도체로 가역적으로 변하는 현상이다. 모트 전이는 약 100 fJ의 초저전력으로 700 ps 내에서 초고속으로 일어나며, 모트 전이 소자는 2 단자의 간단한 MIM (Metal-Insulator-Metal) 구조로 제작될 수 있으므로 고성능 난수 발생기에 적합하다.

본 연구팀은 NbOx 기반의 모트 전이 소자를 성공적으로 제작하고 모트 전이 소자에 부하 저항(load resistor)을 연결하여 자가 진동 회로를 제작하였다.(그림 1, a) 이러한 모트 전이 소자의 진동 거동은 열의 발생과 전달의 무작위성에 의해 확률적 거동을 보이며, 시간이 지남에 따라 이러한 확률적 거동이 누적되면 완전한 무작위성을 구현할 수 있음을 확인했다.(그림 1, b) 본 연구팀은 이러한 확률적 진동 거동 현상이 모트 전이 소자의 진동거동 중 발생하는 줄열의 발생과 소멸이 불연속적임에 기인하며, 이러한 열적 불안전성이 확률적 진동 거동의 원인임을 수치 모사 시뮬레이션과 COMSOL 기반의 열적 시뮬레이션으로 확인했다.(그림 2, a-d)

본 연구팀은 모트 전이 진동 소자가 일정 시간에 동작하는 진동의 횟수가 무작위함을 통해, 이를 홀수와 짝수로 나누어 이진화하는 방식의 진성 난수 발생기 회로를 제시했다.(그림 3) 고안한 진성 난수 발생기는 무작위성을 부여하는 모트 전이 소자 진동 회로, 진동 신호를 증폭하는 operational amplifier, 그리고 진동 횟수를 홀수와 짝수를 구분하고 이를 이진화하는 T flip-flop으로 구성된다. 진성 난수 발생기를 브레드보드에 구성하고, 실제로 구동하여 고안한 진성 난수 발생기가 성공적으로 난수를 발생시킬 수 있음을 확인했다.(그림 4)

## 3. 기대효과

본 연구팀에서 개발한 진성 난수 발생기는 종래 연구에 비해 11배 에너지 효율적이며 (5.22 nJ/bit), 2.5배 빠르며 (40 kb/s), 7.4 배 집적화된 회로에서 진성 난수를 성공적으로 발생시킬 수 있으며, 브레드보드에 구성된 진성 난수 발생기를 통해 130 M bits의 난수를 생성하고 미국 국립표준기술원에서 고안한 NIST 800-22 난수 테스트를 통해 난수 발생기를 검증함으로써 난수 발생기의 성능을 객관적으로 입증했다. (표 1) 또한, 개발한 진성 난수 발생기는 모트 전이 소자 진동 회로의 전위와 저항에 관계없이 진동 거동이 유발되는 한 난수 발생이 가능하며, 따라서 소자의 열화에 강한 난수 발생 기법임. 더해서, 주변 온도가 올라감에 따라 난수 발생 속도는 오히려 증가하며, 많은 양의 정보를 빠른 속도로 암호화하는 상황에서도 고성능을 유지할 수 있다.

표 1. NIST 800-22 난수 테스트 결과.

| NIST test (800-22) | P-value | PASS (if P-value > 0.0001) | Pass rate | Minimum pass rate |
|---|---|---|---|---|
| 1. Frequency (monobit) test | 0.010751 | PASS | 130 / 130 | 125 / 130 |
| 2. Frequency test within a block | 0.451595 | PASS | 128 / 130 | 125 / 130 |
| 3. Runs test | 0.082824 | PASS | 129 / 130 | 125 / 130 |
| 4. Test for the longest run of ones in a block | 0.066882 | PASS | 130 / 130 | 125 / 130 |
| 5. Binary matrix rank test | 0.046361 | PASS | 130 / 130 | 125 / 130 |
| 6. Discrete Fourier transform (spectral test) | 0.001173 | PASS | 128 / 130 | 125 / 130 |
| 7. Non-overlapping template matching test | 0.095249 | PASS | 128 / 130 | 125 / 130 |
| 8. Overlapping template matching test | 0.125088 | PASS | 130 / 130 | 125 / 130 |
| 9. Maurer's "universal statistical" test | 0.017912 | PASS | 130 / 130 | 125 / 130 |
| 10. Linear complexity test | 0.020984 | PASS | 130 / 130 | 125 / 130 |
| 11. Serial test | 0.217681 | PASS | 130 / 130 | 125 / 130 |
| 12. Approximate entropy test | 0.001106 | PASS | 128 / 130 | 125 / 130 |
| 13. Cumulative sums (cusum) test | 0.003951 | PASS | 127 / 130 | 125 / 130 |
| 14. Random excursions test | 0.009640 | PASS | 130 / 130 | 125 / 130 |
| 15. Random excursions variant test | 0.001527 | PASS | 130 / 130 | 125 / 130 |

Total 130×10⁶ binary bits are collected from our NbOx-based oscillation memristor TRNG.

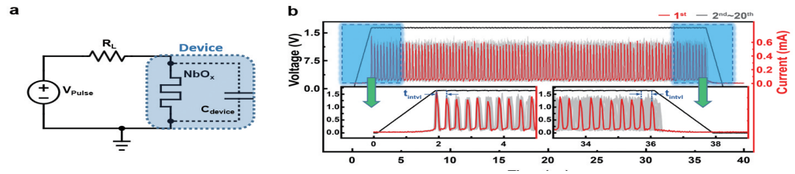


그림 1.
a. 모트 전이 소자 기반 진동 회로
b. 모트 전이 소자의 확률적 진도 거동

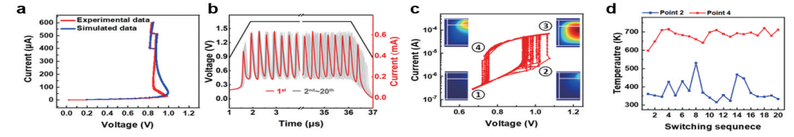


그림 2.
a. 수치 모사 시뮬레이션 기반 모트 전이 소자 특성 모사 및
b. 확률적 진동 거동 모사
c. 열적 시뮬레이션 기반 모트 전이 소자의 확률적 진동 거동 모사 및
d. 진동 거동 중 스위칭 온도

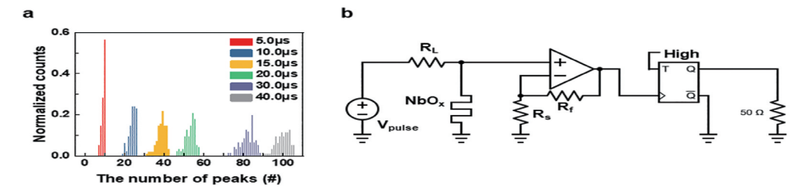


그림 3.
a. 진동 시간에 따른 진도 횟수 분포
b. 진성 난수 발생기 회로

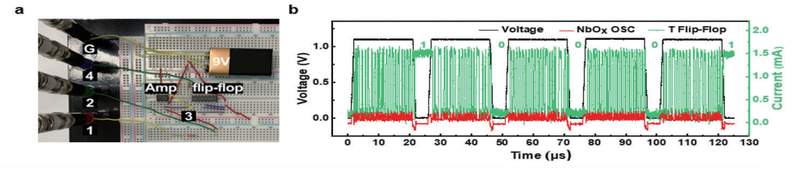


그림 4.
a. 브레드보드에 구성한 진성 난수 발생기
b. 진성 난수 발생기 동작 시연

**연구성과**

- 논문: G. Kim, J. H. In, Y. S. Kim, H. Rhee, W. Park, H. Song, J. Park, and K. M. Kim*, "Self-clocking fast and variation tolerant true random number generator based on a stochastic mott —memristor", Nature Communications, 12, 2906 (2021) [2020 impact factor = 14.919]
- 수상: Self-clocking fast and variation tolerant true random number generator based on a stochastic mott memristor. 제 28회 한국반도체학술대회, 현장우수포스터상 수상.
- 홍보: 언론보도 20여 회

**연구비 지원**

산업자원통상부, 저전력 멤리스터를 이용한 선형성 대칭성 아날로그 시냅스 구현
산업자원통상부, 크로스바 구조에서 선택소자 없이 동작 가능한 자가정류 저항변화 재료 및 소자 개발
한국반도체연구조합, 크로스바 구조에서 선택소자 없이 동작 가능한 자가정류 저항변화 재료 및 소자 개발