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

Principal Investigator
Kyung Min Kim

Department
Department of Material Science and Engineering

Homepage
http://semi.kaist.ac.kr

The intrinsic stochasticity of the memristor can be used to generate true random numbers, essential for non-decryptable hardware-based security devices. Here, we propose a novel and advanced method to generate true random numbers utilizing the stochastic oscillation behavior of a NbOx mott memristor, exhibiting self-clocking, fast and variation tolerant characteristics. The random number generation rate of the device can be at least 40 kb/s, which is the fastest record compared with previous volatile memristor-based TRNG devices. Also, its dimensionless operating principle provides high tolerance against both ambient temperature variation and device-to-device variation, enabling robust security hardware applicable in harsh environments.

1. Background (objectives)

The security system requires TRNG (True Random Number Generator) to encrypt the data. Previous security technologies utilized the TRNG based on CMOS (Complementary metal-oxide-semiconductor) hardware. However, they suffer from low-security levels, large energy consumption, and difficulty in scaling. Accordingly, their use in IoT (Internet of Things) era is challenging, where the small edge devices are connected and communicate. To overcome the limitation of CMOS-based security hardware, researchers have developed the security hardware utilizing the stochastic resistance switching nature in transition metal oxides (e.g., TaOx, HfOx). As such, in future it is crucial to develop a higher operating speed and lower-power consuming TRNG from the stochastic resistance switching nature.

2. Contents

Recent TRNGs utilized diffusive memristors or charge trap memristors to obtain the stochastic behavior. However, their speeds were not sufficiently fast as the switching speeds of those memristors are slow in principle. In this study, we focused on a Mott transition in oxides. Mott transition is a reversible insulator-metal transition requiring low energy (~ 100 fJ) for a short time (~700 ps). Thus, its fast switching may allow a high-speed operation of the TRNG.

We fabricated a NbOx-based Mott device and developed an oscillator circuit composed of a load resistor and the Mott device. (Figure 1, a) The oscillation of the Mott oscillator is stochastic due to the unpredictable thermal fluctuation, which can be regarded as more random over time. (Figure 1, b) We performed numerical multiphysics simulation to confirm the origin of the stochastic oscillation is on the discontinuity in heat generation and dissipation. (Figure 2, a-d)

The next challenge is to extract the random bit from the stochastic device. For that, we designed a TRNG circuit that counts the number of the oscillation peaks, decides whether it is even or odd, and digitalizes it. (Figure 3) It is composed of the Mott oscillator as a random source, an op-amp for oscillation signal amplification, and a T flip-flop which binarizes the number of oscillation peaks. We integrated the TRNG circuit on a breadboard and successfully demonstrated its operation. (Figure 4) Our TRNG can be operated 11 times energy-efficiently (5.22 nJ/bit) at a 2.5 times faster rate (40 kb/s) in 7.4 times scaled area than the previous TRNG. We collected 130 Mbits of random numbers and confirmed its realiable randomness by performing NIST 800-22 randomness test. (Table 1)

3. Expected effect

The energy efficiency, rapid speed, and high scalability of the developed TRNG can be used in edge IoT devices for data encryption. Also, the stochastic behavior can be used for various emerging computing technologies, such as neuromorphic computing and probabilistic computing, Our study revealed a complicated thermal and electrical correlation in mott device, and the origin of its stochastic behavior. This finding can be extended to a high-order multiphysics system and pioneers a new branch of the research field in material science.

Table 1. NIST 800-22 test results

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.

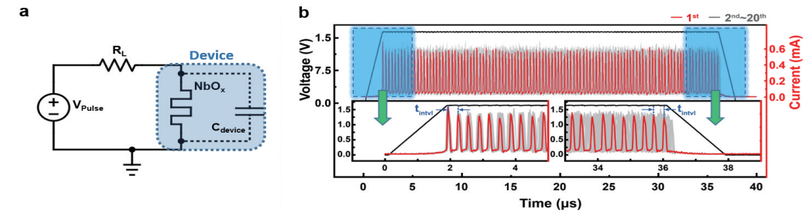

Figure 1.
a. NbO_x Mott device based oscillator circuit
b. The stochastic oscillation of Mott device

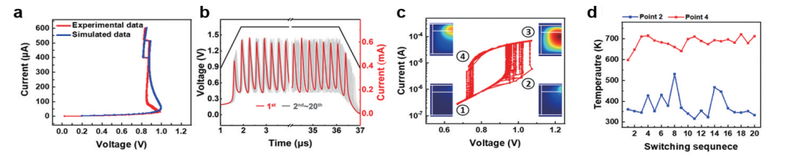

Figure 2.
a. The NDR curve of numerically emulated Mott device, and
b. its stochastic oscillation
c. The I-V curves during stochastic oscillation conducted based on COMSOL simulation.
d. The switching temperature during the oscillation.

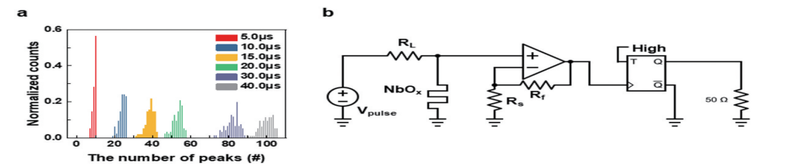

Figure 3.
a. The peak number distribution upon the oscillation time
b. The TRNG circuit based on the stochastic Mott device.

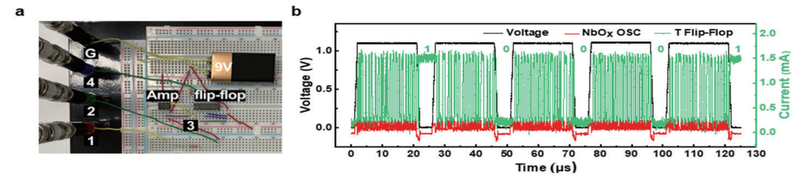

Figure 4.
a. The TRNG circuit integrated on a breadboard.
b. The experimental Idemonstion of the TRNG.

Research outcomes

Paper 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]

Award Excellence poster award at 28th KCS for paper 1

Press release About 20 times media reports for paper 1

Research funding

2020 UP Research Project of KAIST
Ministry of Trade, Industry & Energy, Analog Synapse Devices using low power device with linearity and symmetry.
Ministry of Trade, Industry & Energy, Development of self rectifying resistance switching materials and devices for selectorless crossbar application.
Korea Semiconductor Research Consortium support program for the development of the future semiconductor device