A Random Number Generator based on Insulator-to-Metal Electronic Phase Transitions

Matthew Jerry[1], Abhinav Parihar[2], Arijit Raychowdhury[2], and Suman Datta[1]
[1]*University of Notre Dame, Notre Dame, IN 46556, USA*
[2]*Georgia Institute of Technology, Atlanta, GA 30332, USA*
Email: mjerry@nd.edu / Phone: (574) 631-4393

Introduction: Random number generators (RNG) are a fundamental hardware component in modern cryptographic systems [1]. The generation of random numbers can be subdivided into two classes, pseudo-RNGs and hardware RNGs. In pseudo-RNGs software algorithms are implemented on deterministic hardware but are dependent on a set of initial values or "seed", which reduces the security. In contrast, hardware RNGs generate random numbers from a naturally occurring physical phenomenon, such as thermal noise. However, implementations often suffer from large silicon footprints due to the need to create resistor-amplifier-ADC chains [2] or bias removal circuits [3]. In this work, we experimentally demonstrate a compact and scalable 1T1R based RNG by harnessing the inherent stochasticity in the insulator-to-metal phase transition (IMT) in vanadium dioxide (VO_2).

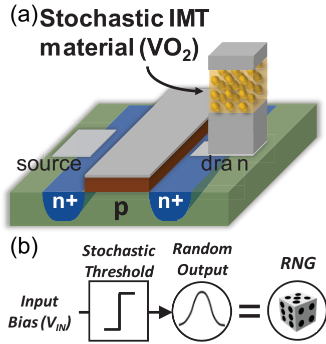
Results: The IMT RNG configuration is shown in Fig. 1(a), where VO_2 is connected in series to the drain side of a MOSFET. The compact design is enabled by the property of bifurcation during the IMT in VO_2, which amplifies the thermal noise, flicker noise, and fluctuation in the IMT trigger voltage (V_{IMT}), while the accompanying MOSFET sets the electrical load-line, reduces static power, and provides input/output isolation. The IMT RNG operating principle is shown in Fig. 2, where the transistor load line is plotted against more than ten DC IV cycles for a single VO_2 device highlighting the stochastic variations in V_{IMT}. While the electrical load line intercepts the unstable arms of the VO_2 DC IV (dashed-line), the VO_2 device oscillates between the insulating and the metallic states, due to the unstable circuit condition, producing voltage spikes at the output (1s) [4]. However, when the transistor load-line intersects the stable insulating arm of the VO_2 DC IV (solid line), the VO_2 device remains in the insulating state and no spikes (0s) occur at the output. Since we design the IMT RNG at the point of bifurcation (Fig. 2), even limited fluctuations in the switching threshold arising from device level stochasticity, lead to a stochastic bit streams at the output. To confirm the DC load line analysis, we perform time domain measurements in Fig. 3. Under a constant input bias at the bifurcation point (V_{IN}=1.92V) spikes (1s) are generated with a probability of ~50% at random time intervals across multiple trials (Fig. 3(c)-(f)), due to the stochastic variations in V_{IMT} as well as additional noise sources. To identify the dominant noise source in the IMT RNG we develop a transient noise model (Fig. 4) which includes V_{IMT} fluctuations ($\Delta V_{IMT}(t)$), flicker noise ($\eta_F(t)$), and thermal noise ($\eta_T(t)$). The model is found to be in excellent agreement with the experimental data as shown by Figs. 5-7, and the results confirm that stochastic fluctuations in V_{IMT} dominate the IMT RNG response. To verify the stochastic variation in V_{IMT} does not result from drift or degradation in the threshold switching voltage, V_{IMT} is plotted as a function of cycle number in Fig. 8(a). V_{IMT} is observed to vary stochastically between 3.4V and 3.7V for all cycles without a reduction in the mean or range [5]. In contrast V_{MIT} variations (fig. 8(b)) are measured to be <±20mV, revealing the large stochastic variations are limited metallic filament formation during the IMT [5]. We characterize the V_{IMT} distributions as a function of device length (Fig. 9) highlighting that the stochasticity is maintained with device scaling. Further, Fig. 10 shows that stochasticity is retained at higher temperature. Finally, we evaluate the performance of the IMT RNG by performing the NIST SP800-22 statistical test for randomness on the measured output waveforms (Fig. 11) [6]. The waveforms are converted to random bit sequences by discretizing time according to the spike periods and classifying presence of spike as 1 and absence as 0. The measured sequences passed all tests with a p-value>0.01, confirming the randomness of the spike sequence (due to the current size of the data vectors block tests were omitted in this study).

Conclusion: In summary, we experimentally demonstrate a compact 1T1R hardware RNG harnessing the inherently stochastic phenomenon of the insulator-to-metal phase transition in VO_2. Through experimentation and modeling we verify the operating principal and scalability of the IMT RNG and validate the randomness of the measured output using the NIST SP800-22 statistical randomness test.

References: [1] M. Bucci, *et. al.*, "A high-speed oscillator-based truly random number source for cryptographic applications on a smartcard IC," *IEEE Trans. Comput.*, 52(4), 2003. [2] C. S. Petrie, *et. al.*, "A noise-based IC random number generator for applications in cryptography," *IEEE Trans. Circuits Syst. I Fundam. Theory Appl.*, 47(5), 2000. [3] C. Tokunaga, *et. al.*, "True Random Number Generator With a Metastability-Based Quality Control," *IEEE J. Solid-State Circuits*, 43(1), 2008. [4] M. Jerry, *et. al.*, "Phase transition oxide neuron for spiking neural networks," *Device Research Conference*, 2016. [5] M. Jerry, *et. al.*, "Dynamics of electrically driven sub-nanosecond switching in vanadium dioxide," *IEEE Silicon Nanoelectronics Workshop (SNW)*, 2016. [6] A. Rukhin, *et. al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," *Natl. Inst. Stand. Technol.*, 800, 2010.

978-1-5090-6328-4/17/$31.00 ©2017 IEEE

Authorized licensed use limited to: Georgia Institute of Technology. Downloaded on June 28,2021 at 15:50:21 UTC from IEEE Xplore. Restrictions apply.



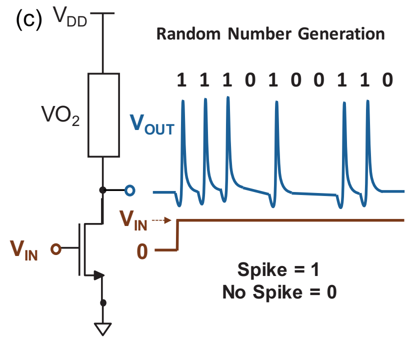


Fig. 1: (a) Device schematic of insulator-to-metal transition (IMT) based random number generator (RNG). (b) Stochasticity in the threshold switching voltage of VO_2 enables probabilistic output. (c) IMT RNG circuit and I/O function.

Fig. 2: Load line operating principal. Probabilistic spiking occurs when the transistor load line intersects the stochastically varying V_{IMT} point .

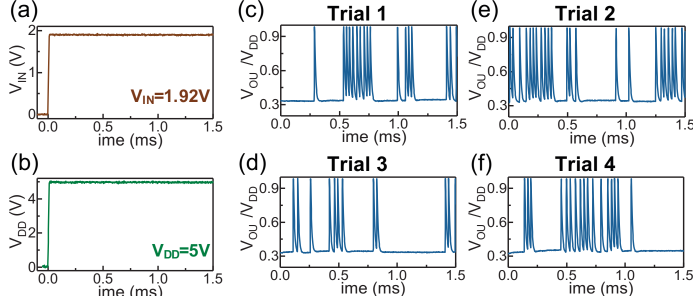


Fig. 3: (a-b) Input (V_{GS}=1.92V) and V_{DD} (5V) bias for IMT RNG. (c-f) Corresponding measured output transients over four trials. IMT RNG produces various random spike sequences due to stochastic fluctuations in V_{IMT}.

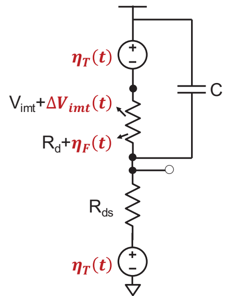


Fig. 4: IMT RNG transient noise model (V_{IMT}, flicker, and thermal noise).

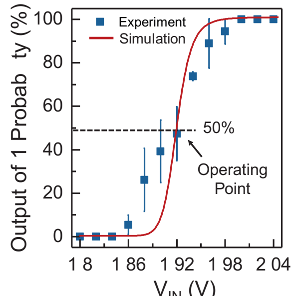


Fig. 5: Measured and simulated probability of IMT RNG output being 1, as function of V_{GS}.

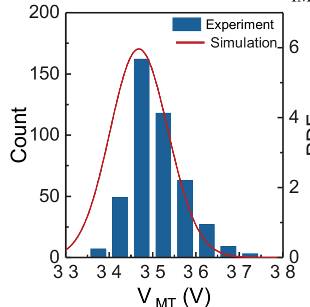


Fig. 6: Extracted V_{IMT} variations from time domain measurements. Solid line shows simulated V_{IMT} PDF from model in Fig. 4.

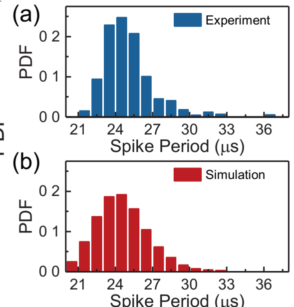


Fig. 7: (a) Measured and (b) simulated spike period distributions highlights the model accuracy.

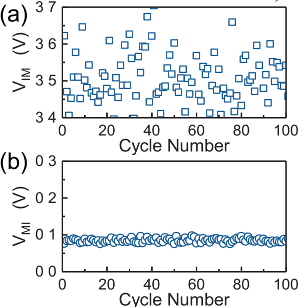


Fig. 8: (a) Measured V_{IMT} variation does not reduce or degrade with cycling. (b) Stochasticity is not observed in the MIT.

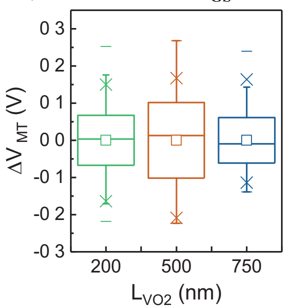


Fig. 9: Measured V_{IMT} stochasticity is observed to be independent of device size. Results are normalized to the mean V_{IMT} value.

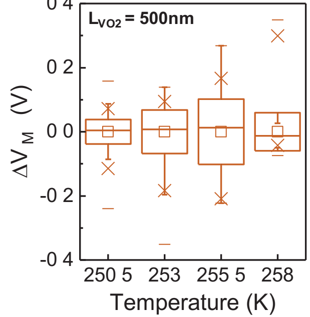


Fig. 10: Temperature dependence of variation in V_{IMT} for L_{VO2} = 500nm device. Stochasticity is retained away from T_C (270K). Distributions are generated from >3000 cycles and normalized to the mean V_{IMT} value.

Test	p-value Data Set 1	p-value Data Set 2
Frequency	0.1281	1.000
Cum. Sum (f)	0.0359	0.4236
Cum. Sum (r)	0.1819	0.4236
FFT	0.3323	0.7026
Run	0.1159	0.0960

Test passed if p>0.01

Fig. 11: Measured NIST SP800-22 randomness test results [5]. P-values greater than 0.01 indicate the sequence is random and the test is passed.

978-1-5090-6328-4/17/$31.00 ©2017 IEEE

Authorized licensed use limited to: Georgia Institute of Technology. Downloaded on June 28,2021 at 15:50:21 UTC from IEEE Xplore. Restrictions apply.