

Stochastic Insulator-to-Metal Phase Transition-Based True Random Number Generator

Matthew Jerry[✉], Student Member, IEEE, Kai Ni[✉], Abhinav Parihar, Arijit Raychowdhury, Senior Member, IEEE, and Suman Datta, Fellow, IEEE

Abstract—An oscillator-based true random number generator (TRNG) is experimentally demonstrated by exploiting inherently stochastic threshold switching in the insulator-to-metal transition (IMT) in vanadium dioxide. Through experimentation and modeling, we show that the origin of stochasticity arises from small perturbations in the nanoscale domain structure, which are then subsequently amplified through a positive feedback process. Within a 1T1R oscillator, the stochastic cycle-to-cycle variations in the IMT trigger voltage result in random timing jitter, which is harnessed for a TRNG. The randomness of the IMT TRNG output is validated using the NIST SP800-22 statistical test.

Index Terms—Truly random number generator, phase-transition, vanadium dioxide, insulator-to-metal transition.

I. INTRODUCTION

RANDOM number generators (RNG) are a fundamental component in modern computational systems used to cryptographically secure stored and transmitted data from eavesdroppers [1]–[3] and recently in machine learning algorithms to regularize networks [4], [5]. With the ever-expanding use of wireless networks, user authentication, and online learning algorithms, the need for compact on-chip, low power, and low cost random number generation is critical. Generating random numbers can be achieved using either pseudo-RNGs or true random number generators (TRNG). Pseudo-RNGs rely on a small set of initial values or “seed” which is subsequently used to compute a larger random sequence using deterministic software algorithms. Due to the

Manuscript received October 17, 2017; revised November 5, 2017; accepted November 6, 2017. Date of publication November 9, 2017; date of current version December 27, 2017. This project was supported by the National Science Foundation under grant 1640081, and the Nanoelectronics Research Corporation (NERC), a wholly-owned subsidiary of the Semiconductor Research Corporation (SRC), through Extremely Energy Efficient Collective Electronics (EXCEL), an SRC-NRI Nanoelectronics Research Initiative under Research Task ID 2698.001 and 2698.002. The review of this letter was arranged by Editor B. S. Doyle. (*Corresponding author: Matthew Jerry*)

M. Jerry, K. Ni, and S. Datta are with the Department of Electrical Engineering, University of Notre Dame, Notre Dame, IN 46556 USA (e-mail: mjerry@nd.edu).

A. Parihar and A. Raychowdhury are with the Department of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332 USA.

Color versions of one or more of the figures in this letter are available online at <http://ieeexplore.ieee.org>.

Digital Object Identifier 10.1109/LED.2017.2771812

deterministic nature of the algorithms, and the dependence on the “seed”, this methodology reduces overall security. In contrast, TRNGs generate random numbers from a naturally occurring physical process, such as thermal or shot noise. This results in a higher level of security as these processes are nondeterministic and cannot be reproduced. Emerging devices such as magnetic tunnel junctions [6] and resistive random access memory devices [7] exhibit intrinsic stochastic behavior and have shown potential as TRNGs. In this work, we experimentally demonstrate that, inherent stochasticity in the threshold switching characteristics of insulator-to-metal transition (IMT) materials [8]–[10] can be harnessed as a technique to engineer TRNGs.

II. RESULTS AND DISCUSSION

We investigate stochasticity in the prototypical phase transition material, vanadium dioxide (VO₂). While previous works have extensively studied the effects of temperature and device size on the DC characteristics [11]–[14], cycle to cycle switching variations are often detrimental to applications in cross-point selectors [15], [16] and steep switching transistors [17]. Therefore, any stochasticity in the phase transition is often attempted to be reduced. We measure the DC characteristics across 100 consecutive cycles and observe large variations in the switching voltage (V_{IMT}), where a mean value of 1.71V with $\sigma = 40\text{mV}$ and a range of 200mV suggest a stochastic transition (Fig. 1(b)). The DC cycling measurements were repeated across multiple devices, yielding similar results, further confirming stochasticity in the switching of VO₂.

To gain insight into the origin of stochasticity in the VO₂ phase transition, we model the device using a 2D heterogeneous resistive network [18], [19]. The VO₂ device is represented as a grid of resistive domains which are independently capable of undergoing an IMT or MIT based on both the local potential and temperature. To determine if a domain should transition based on the local potential, the average voltage drop (ΔV) across the domain is computed [20]. A probability value is then calculated for the insulator-to-metal transition (P_{IMT}) as well as the metal-to-insulator transition (P_{MIT}) [18]–[20].

$$P_{IMT} = e^{-(E_B - q\Delta V/\gamma)/kT} \quad (1)$$

$$P_{MIT} = e^{-(E_B - E_c)/kT} \quad (2)$$

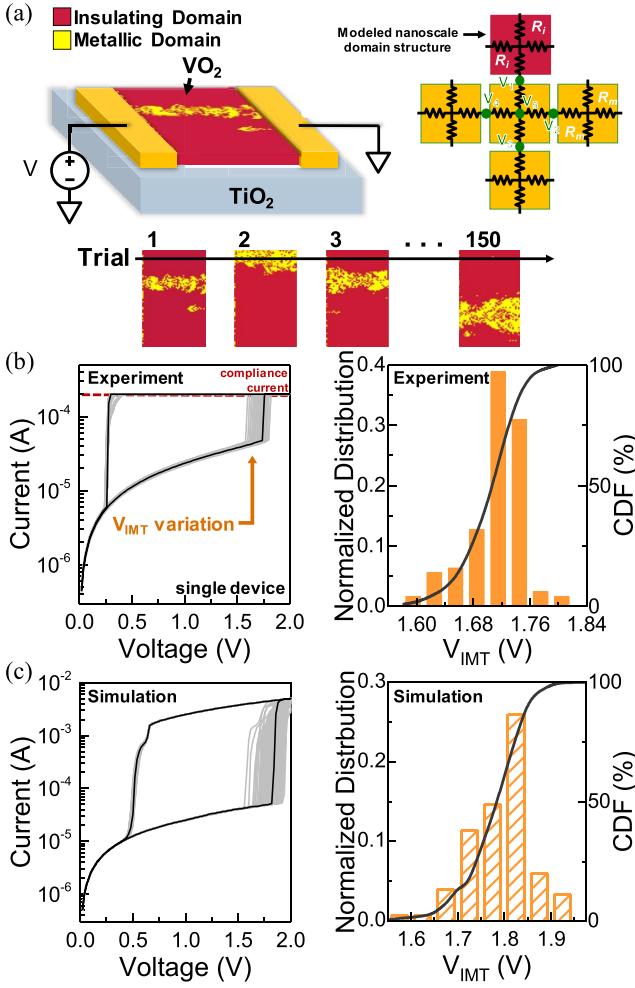


Fig. 1. (a) Electro-thermal 2-D resistive network used to model stochastic variations in VO_2 threshold switching. The variation in V_{IMT} is observed to result from stochastic fluctuations in the nucleation of the metallic filament which is formed through a positive feedback process. (b) Measured DC cycle to cycle variations of V_{IMT} in a single vanadium dioxide device. (c) Simulated variations in V_{IMT} for 150 DC I-V using the 2-D resistive network model.

Additionally, we compute if a domain should undergo thermally activated transition based on the local current flow from equation (3) as given in Janod *et. al.* [21].

$$\frac{\partial T_{n,m}}{\partial t} = p_{n,m} - k \left(4T_{n,m} - \sum_{i}^{\text{1st neighbors}} T_i \right) + h_d(T_{\text{ext}} - T_{n,m}) \quad (3)$$

Simulations are performed by sweeping the source potential at the left boundary of the network and grounding the right (Fig. 1(a)). At each voltage step the domain structure of the network is solved and updated by calculating the potential at every node and computing the individual domain states from equations (1-3). The modelling reveals that the switching event is initiated by an abrupt avalanching process that forms the initial metallic filament, which is in agreement with experimental reports [14], [19]. The abrupt filament formation results from a positive feedback process, wherein the emergence of a small cluster of metallic domains (nucleation point) locally shunts

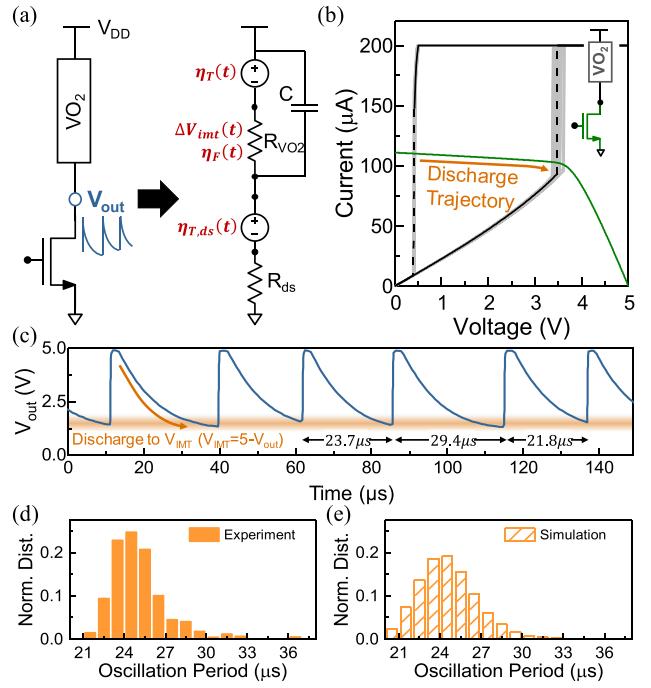


Fig. 2. (a) IMT oscillator and equivalent noise model. (b) Measured load line characteristics highlight the operating principle of the IMT oscillator. (c) Measured time domain waveform. The discharge trajectory is noted as any variations in V_{IMT} result in large changes oscillation period. The normalized distribution of the oscillation period is extracted from >400 (d) measured and (e) simulated oscillation cycles highlighting the large timing jitter.

the current and the voltage drop is redistributed such that a larger potential drop occurs across the remaining insulating domains bridging the two contacts. This creates higher electric fields and increased joule heating in the remaining insulating domains causing them to transition (to the metallic state) and thus abruptly forming the metallic filament. However, since only a small nucleation point is required to induce the IMT, small fluctuations that cause a domain to transition can trigger the IMT. Thus, amplifying any underlying random process and causing the filament formation to occur with spatial and potential variation as well. The authors note that, while the electro-thermal model can correctly capture the experimentally observed dynamics, the fundamental switching physics remain under debate [11], [14], [22]–[24]. Thus, further refinements can be included, as the physics are subsequently revealed.

To exploit this stochastic behaviour for a TRNG, the IMT should be sampled at a high rate. Therefore, we utilize a transistor in series to a VO_2 device (Fig. 2(a)) to provide negative-feedback and form a free running IMT oscillator which maximizes the rate at which the IMT can be sampled. We then bias the oscillator according the load line in Fig. 2(b) and examine the effects of the stochastic thresholding on the oscillator period. Fig. 2(c) shows an example of the oscillator waveform, where the oscillation period is observed to fluctuate stochastically from cycle-to-cycle. This directly results from the variations in V_{IMT} as the discharge cycle of the oscillator is terminated by the IMT (Fig. 2(c)), a point which fluctuates stochastically. Since the discharge cycle dominates the

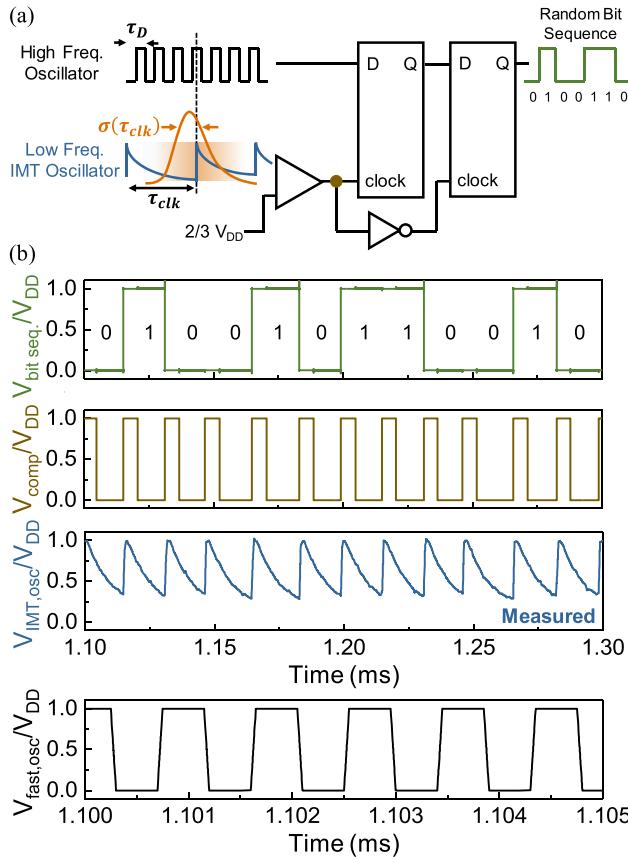


Fig. 3. (a) Block diagram of TRNG based on a stochastic IMT oscillator. (b) Timing diagram of the random bit stream generated by simulating a NAND-based master-slave d flip-flop in Cadence Spectre where the jittery clock is supplied by the experimentally measured IMT oscillator waveform over >87,000 cycles. V_{DD} of the measured IMT oscillator waveform is 5V ($L_{VO_2} = 1\mu m$, $W_{VO_2} = 2\mu m$).

oscillation period, relatively small variations in V_{IMT} result in large variations in the oscillation period (Fig. 2(d)). We further confirm that the V_{IMT} variations are the dominant noise source in the IMT RNG by modeling the oscillator transient with an IMT oscillator noise model [8], [9] 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. 2(d)-(e), and the results confirm that the stochastic fluctuations in V_{IMT} dominate the IMT oscillator response. Therefore, the oscillator jitter is relatively robust to reductions in the magnitude of other noise sources (ex. thermal noise of the transistor) as they are additive to the larger noise due to V_{IMT} fluctuations.

The IMT oscillator TRNG structure is shown in Fig. 3(a) and reflects a standard ring oscillator based TRNG. A high frequency oscillator with 50% duty cycle is input to the data line of a master-slave d flip-flop, while the high jitter IMT oscillator is used as the clock. This results in a random sampling of the data line and produces a random bit-sequence at the output. The circuit is simulated in Cadence Spectre where before the experimentally captured IMT oscillator waveform is applied to the D flip flop clock, it is converted into a rail-to-rail waveform by a comparator (using a Verilog-A model). The random bit

TABLE I
NIST SP800-22 TEST RESULTS

Test	p-value
Frequency	0.088089
Block Frequency	0.763503
Cum. Sum (f)	0.163926
Cum. Sum (r)	0.020628
Runs	0.084915
Longest Run	0.411331
Rank	0.664524
FFT	0.067153
Non-Overlapping Template	144/147
Overlapping Template	0.968964
Serial (P-value ₁)	0.339950
Serial 2 (P-value ₂)	0.100845
Linear Complexity	0.210997
Approximate Entropy	0.135015
Test passed if p>0.01	

sequence is then generated by sampling a 1.113 MHz periodic input signal with the high jitter IMT oscillator clock. The randomness of which is evaluated by performing the NIST SP800-22 [25] statistical test on the >87,000 bits in the output sequence. The output bit sequence is found to pass nearly all tests, indicated in Table 1 by p-values > 0.01, thus confirming the randomness of the sequence over thousands of oscillation periods.

The IMT based TRNG is a device concept that exploits stochasticity in the abrupt threshold switching of IMT materials. Considerations for IMT material choice and optimization should include the fundamental transition speed, switching power, the role of thermal effects on the stochasticity, device area, and fabrication compatibility with CMOS to enable TRNGs based on compact 1T1R IMT oscillators. Although the performance in the current VO₂ based demonstration is limited by the large device size ($L_{VO_2} = 1\mu m$, $W_{VO_2} = 2\mu m$) and the bit rate by the RC limited IMT oscillator frequency. As the VO₂ device size is scaled and directly integrated with the transistor [26], the ability to electrically induce the IMT at sub-nanosecond speeds [18] and operate IMT oscillators at below 1V V_{DD} [8], provides a promising path forward.

III. CONCLUSION

In summary, we experimentally demonstrated a TRNG that utilizes the large timing jitter exhibited in VO₂ oscillators enabled by inherent stochasticity in the insulator-to-metal phase transition. Through experimentation and modeling, we revealed the stochasticity to originate from the amplification of small perturbations within the nanoscale domain structure by the positive feedback process of the IMT. The randomness of the IMT TRNG is validated on the NIST SP800-22 statistical randomness test.

REFERENCES

- [1] C. S. Petrie and J. A. Connelly, "A noise-based IC random number generator for applications in cryptography," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 47, no. 5, pp. 615–621, May 2000, doi: [10.1109/81.847868](https://doi.org/10.1109/81.847868).

- [2] S. K. Mathew, D. Johnston, S. Satpathy, V. Suresh, P. Newman, M. A. Anders, H. Kaul, A. Agarwal, S. K. Hsu, G. Chen, and R. K. Krishnamurthy, “ μ RNG: A 300–950 mV, 323 Gbps/W all-digital full-entropy true random number generator in 14 nm FinFET CMOS,” *IEEE J. Solid-State Circuits*, vol. 51, no. 7, pp. 1695–1704, Jul. 2016, doi: [10.1109/JSSC.2016.2558490](https://doi.org/10.1109/JSSC.2016.2558490).
- [3] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanouovo, “A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC,” *IEEE Trans. Comput.*, vol. 52, no. 4, pp. 403–409, Apr. 2003, doi: [10.1109/TC.2003.1190581](https://doi.org/10.1109/TC.2003.1190581).
- [4] S. Sheik, S. Paul, C. Augustine, C. Kothapalli, M. M. Khellah, G. Cauwenberghs, and E. Neftci, “Synaptic sampling in hardware spiking neural networks,” in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2016, pp. 2090–2093, doi: [10.1109/ISCAS.2016.7538991](https://doi.org/10.1109/ISCAS.2016.7538991).
- [5] L. Wan, M. Zeiler, S. Zhang, Y. Le Cun, and R. Fergus, “Regularization of neural networks using DropConnect,” in *Proc. 30th Int. Conf. Mach. Learn. (ICML)*, 2013, pp. 1058–1066.
- [6] W. H. Choi, Y. Lv, J. Kim, A. Deshpande, G. Kang, J.-P. Wang, and C. H. Kim, “A magnetic tunnel junction based true random number generator with conditional perturb and real-time output probability tracking,” in *IEDM Tech. Dig.*, Dec. 2014, pp. 12.5.1–12.5.4, doi: [10.1109/IEDM.2014.7047039](https://doi.org/10.1109/IEDM.2014.7047039).
- [7] S. Balatti, S. Ambrogio, Z. Wang, and D. Ielmini, “True random number generation by variability of resistive switching in oxide-based devices,” *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 5, no. 2, pp. 214–221, Jun. 2015, doi: [10.1109/JETCAS.2015.2426492](https://doi.org/10.1109/JETCAS.2015.2426492).
- [8] M. Jerry, A. Parihar, B. Grisafe, A. Raychowdhury, and S. Datta, “Ultra-low power probabilistic IMT neurons for stochastic sampling machines,” in *Proc. Symp. VLSI Technol.*, vol. 8, 2017, pp. T186–T187, doi: [10.23919/VLSIT.2017.7998148](https://doi.org/10.23919/VLSIT.2017.7998148).
- [9] M. Jerry, A. Parihar, A. Raychowdhury, and S. Datta, “A random number generator based on insulator-to-metal electronic phase transitions,” in *Proc. 75th Annu. Device Res. Conf. (DRC)*, Jun. 2017, pp. 1–2, doi: [10.1109/DRC.2017.7999423](https://doi.org/10.1109/DRC.2017.7999423).
- [10] A. A. Sharma, Y. Kesim, M. Shulaker, C. Kuo, C. Augustine, H. S.-P. Wong, S. Mitra, M. Skowronski, J. A. Bain, and J. A. Weldon, “Low-power, high-performance S-NDR oscillators for stereo (3D) vision using directly-coupled oscillator networks,” in *Proc. IEEE Symp. VLSI Technol.*, Jun. 2016, pp. 1–2, doi: [10.1109/VLSIT.2016.7573438](https://doi.org/10.1109/VLSIT.2016.7573438).
- [11] J. Cao, W. Fan, K. Chen, N. Tamura, M. Kunz, V. Eyert, and J. Wu, “Constant threshold resistivity in the metal-insulator transition of VO₂,” *Phys. Rev. B, Condens. Matter*, vol. 82, no. 24, p. 241101(R), Dec. 2010, doi: [10.1103/PhysRevB.82.241101](https://doi.org/10.1103/PhysRevB.82.241101).
- [12] A. A. Stabile, S. K. Singh, T.-L. Wu, L. Whittaker, S. Banerjee, and G. Sambandamurthy, “Separating electric field and thermal effects across the metal-insulator transition in vanadium oxide nanobeams,” *Appl. Phys. Lett.*, vol. 107, no. 1, p. 013503, Jul. 2015, doi: [10.1063/1.4926334](https://doi.org/10.1063/1.4926334).
- [13] Y. Zhou, X. Chen, C. Ko, Z. Yang, C. Mouli, and S. Ramanathan, “Voltage-triggered ultrafast phase transition in vanadium dioxide switches,” *IEEE Electron Device Lett.*, vol. 34, no. 2, pp. 220–222, Feb. 2013, doi: [10.1109/LED.2012.2229457](https://doi.org/10.1109/LED.2012.2229457).
- [14] A. Zimmers, L. Aigouy, M. Mortier, A. Sharoni, S. Wang, K. G. West, J. G. Ramirez, and I. K. Schuller, “Role of thermal heating on the voltage induced insulator-metal transition in VO₂,” *Phys. Rev. Lett.*, vol. 110, no. 5, p. 056601, Jan. 2013, doi: [10.1103/PhysRevLett.110.056601](https://doi.org/10.1103/PhysRevLett.110.056601).
- [15] K. Zhang, B. Wang, F. Wang, Y. Han, X. Jian, H. Zhang, and H. S. P. Wong, “VO₂-based selection device for passive resistive random access memory application,” *IEEE Electron Device Lett.*, vol. 37, no. 8, pp. 978–981, Aug. 2016, doi: [10.1109/LED.2016.2582259](https://doi.org/10.1109/LED.2016.2582259).
- [16] M. Son, J. Lee, J. Park, J. Shin, G. Choi, S. Jung, W. Lee, S. Kim, S. Park, and H. Hwang, “Excellent selector characteristics of nanoscale VO₂ for high-density bipolar ReRAM applications,” *IEEE Electron Device Lett.*, vol. 32, no. 11, pp. 1579–1581, Nov. 2011, doi: [10.1109/LED.2011.2163697](https://doi.org/10.1109/LED.2011.2163697).
- [17] E. A. Casu, W. A. Vitale, N. Oliva, T. Rosca, A. Biswas, C. Alper, A. Krammer, G. V. Luong, Q. T. Zhao, S. Mantl, A. Schuler, A. Seabaugh, and A. M. Ionescu, “Hybrid phase-change–Tunnel FET (PC-TFET) switch with subthreshold swing < 10 mV/decade and sub-0.1 body factor: Digital and analog benchmarking,” in *IEDM Tech. Dig.*, Dec. 2016, pp. 19.3.1–19.3.4, doi: [10.1109/IEDM.2016.7838452](https://doi.org/10.1109/IEDM.2016.7838452).
- [18] M. Jerry, N. Shukla, H. Paik, D. G. Schlom, and S. Datta, “Dynamics of electrically driven sub-nanosecond switching in vanadium dioxide,” in *Proc. IEEE Silicon Nanoelectronics Workshop (SNW)*, Jun. 2016, pp. 26–27, doi: [10.1109/SNW.2016.7577968](https://doi.org/10.1109/SNW.2016.7577968).
- [19] H. Madan, M. Jerry, A. Pogrebnyakov, T. Mayer, and S. Datta, “Quantitative mapping of phase coexistence in Mott–Peierls insulator during electronic and thermally driven phase transition,” *ACS Nano*, vol. 9, no. 2, pp. 2009–2017, Feb. 2015, doi: [10.1021/nm507048d](https://doi.org/10.1021/nm507048d).
- [20] P. Stolić, L. Cario, E. Janod, B. Corraze, C. Guillot-Deudon, S. Salmon-Bourmand, V. Guiot, J. Tranchant, and M. Rozenberg, “Universal electric-field-driven resistive transition in narrow-gap Mott insulators,” *Adv. Mater.*, vol. 25, no. 23, pp. 3222–3226, Jun. 2013, doi: [10.1002/adma.20130113](https://doi.org/10.1002/adma.20130113).
- [21] E. Janod, J. Tranchant, B. Corraze, M. Querré, P. Stolić, M. Rozenberg, T. Cren, D. Roditchev, V. T. Phuoc, M.-P. Besland, and L. Cario, “Resistive switching in Mott insulators and correlated systems,” *Adv. Funct. Mater.*, vol. 25, no. 40, pp. 6287–6305, Oct. 2015, doi: [10.1002/adfm.201500823](https://doi.org/10.1002/adfm.201500823).
- [22] A. B. Pevtsov, A. V. Medvedev, D. A. Kurdyukov, N. D. Il’inskaya, V. G. Golubev, and V. G. Karpov, “Evidence of field-induced nucleation switching in opal: VO₂ composites and VO₂ films,” *Phys. Rev. B, Condens. Matter*, vol. 85, no. 2, p. 024110, Jan. 2012, doi: [10.1103/PhysRevB.85.024110](https://doi.org/10.1103/PhysRevB.85.024110).
- [23] S. Rathi, J.-H. Park, I.-Y. Lee, J. M. Baik, K. S. Yi, and G.-H. Kim, “Unravelling the switching mechanisms in electric field induced insulator–metal transitions in VO₂ nanobeams,” *J. Phys. D, Appl. Phys.*, vol. 47, no. 29, p. 295101, Jul. 2014, doi: [10.1088/0022-3727/47/29/295101](https://doi.org/10.1088/0022-3727/47/29/295101).
- [24] T. Driscoll, J. Quinn, M. Di Ventra, D. N. Basov, G. Seo, Y.-W. Lee, H.-T. Kim, and D. R. Smith, “Current oscillations in vanadium dioxide: Evidence for electrically triggered percolation avalanches,” *Phys. Rev. B, Condens. Matter*, vol. 86, no. 9, p. 094203, Sep. 2012, doi: [10.1103/PhysRevB.86.094203](https://doi.org/10.1103/PhysRevB.86.094203).
- [25] L. E. Bassham, A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, N. Heckert, J. Dray, and S. Vo, “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep., 2010. [Online]. Available: <https://dl.acm.org/citation.cfm?id=2206233>, doi: [10.6028/NIST.SP.800-22r1a](https://doi.org/10.6028/NIST.SP.800-22r1a).
- [26] J. Frougier, N. Shukla, D. Deng, M. Jerry, A. Aziz, L. Liu, G. Lavallee, T. S. Mayer, S. Gupta, and S. Datta, “Phase-transition-FET exhibiting steep switching slope of 8 mV/decade and 36% enhanced ON current,” in *Dig. Tech. Papers-Symp. VLSI Technol.*, Jun. 2016, pp. 1–2, paper JFS4-3, doi: [10.1109/VLSIT.2016.7573445](https://doi.org/10.1109/VLSIT.2016.7573445).