# Random Number Generation by Differential Read of Stochastic Switching in Spin-Transfer Torque Memory

Roberto Carboni, *Student Member, IEEE*, Wei Chen, Manzar Siddik, Jon Harms, Andy Lyle, Witold Kula, Gurtej Sandhu, and Daniele Ielmini, *Senior Member, IEEE*

***Abstract*— The true random number generator (TRNG) is a key enabling technology for cryptography and hardware authentication, which are becoming essential features in the era of the Internet of Things (IoT). Here, we present a novel TRNG concept based on the stochastic switching in spin-transfer torque magnetic random access memory (STT-MRAM). The new methodology relies on the STT-MRAM switching variations affecting the current response under applied rectangular or triangular pulses. Random numbers are extracted from the differential read of the integrated current across two stochastic switching cycles. The proposed concept passes all tests in the NIST SP-800-22 suite with no post-processing, thus supporting STT-MRAM as a promising technology for data/hardware security in the IoT.**

***Index Terms*— Spin-transfer torque magnetic memory (STT-MRAM), true random number generator (TRNG), magneto-tunnel junction (MTJ), switching variability, nonvolatile.**

## I. Introduction

THE random number generator (RNG) plays a key role in enabling secure data transmissions [1], [2] by generating random cryptographic keys. The widespread diffusion of internet-based communicating devices and internet of things (IoT) raises the need for compact and reliable RNG circuits, generating random numbers with high entropy and high throughput [3]. In addition, since emerging computing paradigms, such as stochastic [4], [5] and brain-inspired computing [6], [7], require large amounts of random bit sequence [8], they could benefit from a small yet effective random number source. In most cases, random bits are generated via pseudo RNG (PRNG), consisting in software algorithms generating random numbers via a deterministic function of a seed, e.g., the system clock [9]. However, these systems feature limited randomness and can be easily attacked [10]. Data protection against cyberattacks is achieved only with true RNG (TRNG), whose output random sequence comes from inherently-stochastic physical processes [11]. Their unpredictability makes hardware-based TRNG more reliable than software-based PRNG [12], [13]. Possible entropy sources for TRNG are the random telegraph noise (RTN) in dielectrics [14], [15], quantum processes [11], spintronics phenomena [16], [17] and memristive devices [18]–[20]. In TRNG, the entropy source is usually the intrinsic variability of the switching parameters, such as resistance and set/reset voltages [21], [22]. Both spin-transfer torque magnetic memory (STT-MRAM) [16], [23] and RRAM [18]–[20] have been used to demonstrate working TRNG. A significant drawback in these techniques is their need for a probability tracking scheme to determine operative voltages for uniform TRNG, i.e., equal probability of generating 0 and 1 [20], [24]. Recently, a differential approach using 2 RRAM devices has been proposed to avoid the need for probability tracking and its associated circuit and algorithm overhead [20]. However, such a differential scheme requires a relatively low mismatch between the switching characteristics in the differential pair.

Here, we report a novel methodology for physical unbiased generation of true random numbers based on the stochastic switching time of STT [21]. A differential scheme is adopted by comparing the switching characteristics of the same device over 2 consecutive cycles with either rectangular or triangular pulses. The new RNG concept is finally validated against the NIST SP-800-22 test suite [25], with no post-processing.

## II. STT-MRAM Switching Characteristics

We considered STT-MRAM devices based on a magneto-tunnel junction (MTJ) structure with perpendicular magnetic anisotropy (PMA), as shown in Fig. 1(a) [26]. The MTJ consists of CoFeB pinned layer (PL) and free layer (FL), acting as bottom electrode (BE) and top electrode (TE), respectively, separated by a crystalline MgO dielectric layer. As schematically shown by the energy diagram of Fig. 1(b), the device has 2 stable states, where the magnetic polarization in the FL is either parallel (P) to the PL, corresponding to a low resistance of the MTJ, or antiparallel (AP) state to the PL, corresponding to a high resistance of the MTJ [26], [27]. Fig. 1(c) shows the measured current-voltage (I-V) characteristics, which was obtained by applying triangular positive/negative voltage pulses to the TE

Manuscript received April 14, 2018; accepted May 2, 2018. Date of publication May 11, 2018; date of current version June 26, 2018. This work was supported by the European Research Council under Grant ERC-2014-CoG-648635-RESCUE. The review of this letter was arranged by Editor B. Govoreanu. *(Corresponding author: Daniele Ielmini.)*

R. Carboni and D. Ielmini are with the Dipartimento di Elettronica, Informazione e Bioingegneria and the Italian Universities Nanoelectronics Team, Politecnico di Milano, 20133 Milan, Italy (e-mail: daniele.ielmini@polimi.it).

W. Chen was with Micron Technology, Inc., Boise, ID 83707 USA. He is now with Spin Transfer Technologies, Fremont, CA 94538 USA.

M. Siddik, J. Harms, A. Lyle, and G. Sandhu are with Micron Technology, Inc., Boise, ID 83707 USA.

W. Kula was with Micron Technology, Inc., Boise, ID 83707 USA. He is now with Antaios, SAS, 38330 Montbonnot-Saint-Martin, France.

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.2018.2833543

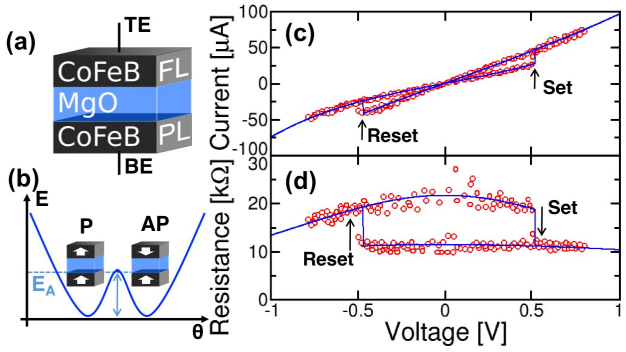


Fig. 1. (a) STT-MRAM device used in this work. (b) Energy as a function of the FL magnetic polarization direction with respect to the PL, evidencing stable P and AP states. (c) Measured and calculated I-V and (d) R-V characteristics, indicating set (AP to P) and reset (P to AP) transitions. The characteristics were obtained under 1 $\mu$s triangular voltage pulses.

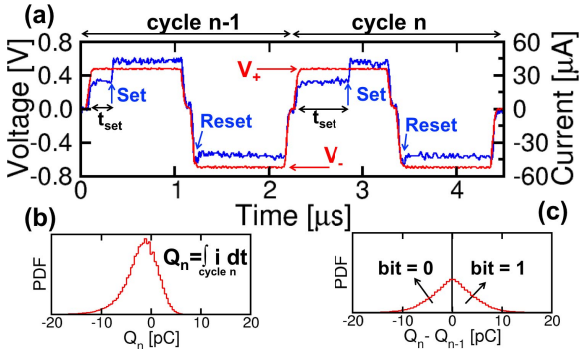


Fig. 2. (a) Measured rectangular voltage pulses and current response for 2 consecutive cycles n − 1 and n, (b) PDF of the integrated current $Q_n$ and (c) PDF of differential charge $\Delta Q_n = Q_n - Q_{n-1}$. The pulse sequence includes positive and negative rectangular pulses for stochastic set and reset transitions, respectively, as evidenced by the abrupt steps in the current response. The random bit is assigned from the value of $\Delta Q_n$ in (c).

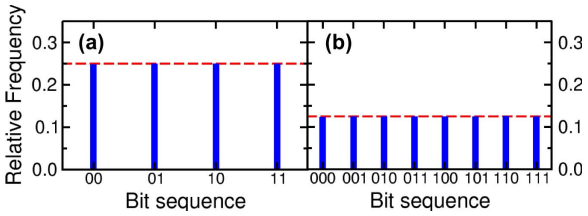


Fig. 3. Relative occurrence of 2-bit (a) and 3-bit sequences (b) for $V_+ = 0.5$ V and $V_- = 0.7$ V. Data show uniform distribution of sequences, with equal probabilities of 0.25 and 0.125 for the 2 and 3-bit sequences, respectively.

with pulse-width 1$\mu$s, and collecting the current response from an oscilloscope [26]. Fig. 1(d) shows the corresponding resistance-voltage (R-V) characteristics, demonstrating AP-to-P (set) transition at the positive set voltage $V_{set}$, and P-to-AP (reset) transition at the negative reset voltage $V_{reset}$. Calculations based on a compact model for STT-MRAM are reported in the figure, showing a good agreement with data [26].

## III. STT-MRAM Based TRNG

The switching event in STT-MRAM is inherently-stochastic, i.e., $V_{set}$ and $V_{reset}$ changes from cycle to cycle [21], [22]. The statistical variation was explained in terms of a thermally-assisted magnetization reversal [28], where the transition from P to AP (or vice versa) arises from a random thermal fluctuation of the FL polarization within the potential well of Fig. 1(b), eventually causing the stochastic transition over the energy barrier $E_A$. As a result, for any applied voltage $V_A > 0$, there exists a statistical distribution of set times $t_{set}$, namely the time delay between the application of $V_A$ and the set transition [21]. Similarly, there is a distribution of reset times $t_{reset}$ measuring the time delay between the application of a voltage $V_A < 0$ and the reset transition.

The variation of switching voltage and/or time was used as the entropy source in previous TRNG concepts [16], [17]. However, these schemes adopt a probability tracking approach to ensure TRNG uniformity. Differential schemes can generate random numbers with no need for probability tracking from the competition between 2 devices, although suffering from the device-to-device mismatch of the switching voltage [20].

To solve this issue, here we adopt a differential scheme, where the device responses over 2 consecutive cycles are compared to yield a random bit. Fig. 2(a) shows the applied voltage and the current response in 2 consecutive cycles. In each cycle, a positive stochastic pulse of voltage $V_+$ is applied, followed by a negative deterministic pulse of voltage $V_-$. Both pulses have a duration $t_P = 1$ $\mu$s. Note that the positive current response during the cycle n − 1 differs from cycle n, namely, the set time $t_{set}$ during cycle n − 1 is shorter than in cycle n as a result of the stochastic AP - P transition. The random bit is generated by comparing the integrated current in the 2 successive cycles of the same STT-MRAM device. Fig. 2(b) shows the experimental probability distribution function (PDF) of the integrated current $Q_n = \int i\ dt$. The measured difference $\Delta Q_n = Q_n - Q_{n-1}$ shows a symmetric PDF in Fig. 2(c), with equal portions of positive and negative $\Delta Q_n$. Therefore, $\Delta Q_n$ is chosen as the statistical variable for generating the random bit, with the bit assigned to 0 or 1 for $\Delta Q_n < 0$ or $\Delta Q_n > 0$, respectively. The symmetric PDF in Fig. 2(c) ensures the uniformity of the generated bit with equal probabilities of the bit being 0 or 1. To further support the TRNG uniformity, Fig. 3 shows the probability of the occurrence of 2-bit sequences (a) and 3-bit sequences (b), indicating equal probabilities of 0s and 1s. Similar TRNG concepts with MTJ rely on whitening algorithms, such as the Von Neumann correction [23] or the XOR operation [8], to obtain a sufficiently uniform bit stream. On the other hand, no post-processing technique is used in the present concept, thus contributing to minimizing the energy and area overhead of the TRNG.

The same methodology is shown in Fig. 4, for triangular applied pulses instead of rectangular pulses. The current response in Fig. 4(a) shows variable set and reset currents. Integrating the current leads to the stochastic charge $Q_n$ in Fig. 4(b), while Fig. 4(c) shows the symmetric distribution of the charge difference $\Delta Q_n$, supporting TRNG with triangular pulses. Note that the TRNG pulse-width can be much faster than 1 $\mu$s used in Figs. 2 and 4, since sub-nanosecond switching was reported for STT-MRAM [29]. A shorter time might allow for a higher TRNG throughput and a smaller $Q_n$, hence a correspondingly smaller area of the integrating capacitor. Also, thanks to the differential read, our concept is reasonably immune from any external biasing effect, such as the application of an external magnetic

TABLE I

NIST TEST RESULTS FOR A SEQUENCE OF MORE THAN 1 Mb OBTAINED FROM RECTANGULAR AND TRIANGULAR PULSES FOR DIFFERENT APPLIED VOLTAGES. SEQUENCES WERE DIVIDED IN 55 SEGMENTS. TEST ARE PASSED IF $P_T > 0.0001$ AND PROPORTION $\geq 52/55$

| **Applied Pulse** | **Rect. $V_+$=0.43V** | | **Rect. $V_+$=0.57V** | | **Rect. $V_+$=0.67V** | | **Tri. $V_+$=0.5V** | | **Tri. $V_+$=0.57V** | | **Tri. $V_+$=0.73V** | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Test** | **$P_T$ value** | **Prop.** | **$P_T$ value** | **Prop.** | **$P_T$ value** | **Prop.** | **$P_T$ value** | **Prop.** | **$P_T$ value** | **Prop.** | **$P_T$ value** | **Prop.** |
| Frequency | 0.014550 | 55/55 | 0.437274 | 55/55 | 0.021999 | 50/55 | 0.401199 | 55/55 | 0.334538 | 55/55 | 0.401199 | 54/55 |
| Block Frequency | 0.002203 | 53/55 | 0.048716 | 55/55 | 0.000000 | 53/55 | 0.000216 | 52/55 | 0.010988 | 52/55 | 0.004629 | 53/55 |
| Cumul. Sums - 1 | 0.000026 | 55/55 | 0.401199 | 55/55 | 0.000883 | 50/55 | 0.334538 | 55/55 | 0.162606 | 55/55 | 0.304126 | 53/55 |
| Cumul. Sums - 2 | 0.003996 | 55/55 | 0.014550 | 55/55 | 0.000253 | 50/55 | 0.834308 | 55/55 | 0.090936 | 54/55 | 0.437274 | 54/55 |
| Runs | 0.000000 | 45/55 | 0.002559 | 55/55 | 0.000648 | 50/55 | 0.000274 | 54/55 | 0.304126 | 53/55 | 0.678686 | 55/55 |
| Longest Run | 0.474986 | 55/55 | 0.042808 | 54/55 | 0.474986 | 55/55 | 0.062821 | 54/55 | 0.554420 | 55/55 | 0.162606 | 55/55 |
| Rank | 0.000026 | 52/55 | 0.304126 | 55/55 | 0.025193 | 54/55 | 0.048716 | 54/55 | 0.719747 | 54/55 | 0.554420 | 55/55 |
| FFT | 0.224821 | 52/55 | 0.759756 | 55/55 | 0.514124 | 54/55 | 0.275709 | 54/55 | 0.162606 | 54/55 | 0.062821 | 55/55 |
| Non-overl. templ. | 45/148 | 5/148 | 148/148 | 145/148 | 55/148 | 8/148 | 148/148 | 143/148 | 148/148 | 148/148 | 148/148 | 147/148 |
| Approx Entropy | 0.145326 | 52/55 | 0.071177 | 55/55 | 0.002203 | 46/55 | 0.025193 | 55/55 | 0.012650 | 53/55 | 0.025193 | 55/55 |
| Serial - 1 | 0.024550 | 52/55 | 0.145326 | 55/55 | 0.000082 | 50/55 | 0.401199 | 55/55 | 0.719747 | 53/55 | 0.595549 | 54/55 |
| Serial - 2 | 0.946308 | 55/55 | 0.304126 | 55/55 | 0.003996 | 55/55 | 0.514124 | 55/55 | 0.304126 | 53/55 | 0.334538 | 55/55 |

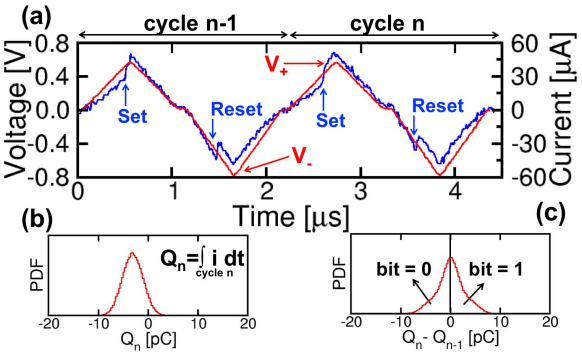


Fig. 4. (a) Measured triangular voltage pulses and current response for 2 consecutive cycles n − 1 and n, (b) PDF of the integrated current $Q_n$ and (c) PDF of differential charge $\Delta Q_n = Q_n - Q_{n-1}$. The pulse sequence includes positive and negative triangular pulses for stochastic set and reset transitions, respectively, as evidenced by the abrupt steps in the current response. The random bit is assigned from the value of $\Delta Q_n$ in (c).

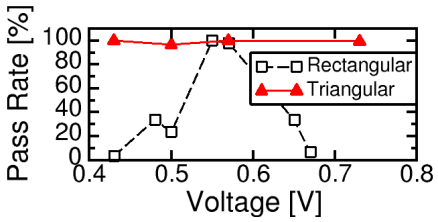


Fig. 5. Pass rate of the non-overlapping template NIST test as a function of pulse voltage for rectangular and triangular pulses. The pass rate is referred to a total of 148 tests. Rectangular pulses show an operation window around 0.6 V, whereas triangular pulses show voltage-independent high randomness.

field or a change in temperature. In fact, the external bias would only affect the switching threshold, but not its cycle-to-cycle variability, which is the key entropy source in the proposed TRNG.

## IV. RANDOMNESS ANALYSIS

To validate a TRNG concept, evaluation of the randomness is mandatory. To this purpose, a industry standard statistical test suite for randomness qualification, namely the NIST SP-800-22 test [25], was applied to our TRNG scheme for a wide variety of pulse amplitude $V_+$, for both rectangular and triangular pulses. Tab. I shows the detailed NIST test output for 3 different voltages for both rectangular and triangular pulses. Although overall results indicate a good randomness, rectangular pulses show failure of some tests at relatively low or high voltages, with best results being achieved within a narrow $V_+$ window. On the other hand, randomness of the triangular case remains high for all the applied voltages. Fig. 5 summarizes the NIST test results by showing the pass rate for the non-overlapping template test. Results indicate the generally good performance with the triangular pulse scheme, and the existence of an optimum window for the rectangular pulse scheme. Results in Fig. 5 can be explained by the dependence on $V_A$ of the stochastic parameters $t_{set}$ and $V_{set}$ for rectangular and triangular pulses, respectively. For a rectangular pulse, the set time $t_{set}$ can be written as [30]:

$$t_{set} = \tau_0 \exp\left(\Delta\left(1 - \frac{V}{V_0}\right)\right), \tag{1}$$

where $V_A$ and $\tau_0$ are constants, V is the applied voltage ($V = V_A$), and $\Delta$ is the thermal stability factor. Given the exponential dependence in Eq. (1), and since the switching time $t_{set}$ should be comparable to the pulse width $t_P$ in Fig. 2, there is a relatively narrow window of $V_A$ for which the entropy is high. On the other hand, for a triangular pulse with ramped voltage according to $V = 2V_A t/t_P$, the set voltage can be estimated by integrating the switching probability according to $\int 1/t_{set}\, dt = 1$, with $t_{set}$ given by Eq. (1). The set voltage along the triangular pulse is thus given by [28], [31]:

$$V_{set} \approx V_0 \ln \frac{t_0 V_A}{V_0 t_P}. \tag{2}$$

indicating a logarithmic dependence of $V_{set}$ on the maximum applied voltage $V_A$. This explains the much smaller dependence of entropy on $V_A$ with respect to the rectangular pulse in Fig. 5.

## V. CONCLUSIONS

A new TRNG based on the stochastic switching time in a STT-MRAM is presented. Purely white random bits are generated from the comparison of the current response over 2 consecutive set/reset cycles. Statistical NIST tests demonstrate the excellent randomness of the output bit-stream, with no need for whitening processes. For triangular pulses, no tracking process is also needed. Due to the simple implementation, high endurance, high scalability and CMOS compatibility of the STT-MRAM, the proposed TRNG is a promising tool for data and hardware security in IoT systems.

## REFERENCES


[1] S. K. Mathew, S. Srinivasan, M. A. Anders, H. Kaul, S. K. Hsu, F. Sheikh, A. Agarwal, S. Satpathy, and R. K. Krishnamurthy, "2.4 Gbps, 7 mW all-digital PVT-variation tolerant true random number generator for 45 nm CMOS high-performance microprocessors," *IEEE J. Solid-State Circuits*, vol. 47, no. 11, pp. 2807–2821, Nov. 2012, doi: 10.1109/JSSC.2012.2217631.

[2] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1996.

[3] S. Ghosh, "Spintronics and security: Prospects, vulnerabilities, attack models, and preventions," *Proc. IEEE*, vol. 104, no. 10, pp. 1864–1893, Oct. 2016, doi: 10.1109/JPROC.2016.2583419.

[4] A. Alaghi and J. P. Hayes, "Survey of stochastic computing," *ACM Trans. Embed. Comput. Syst.*, vol. 12, no. 2S, pp. 92:1–92:19, May 2013, doi: 10.1145/2465787.2465794.

[5] J. S. Friedman, L. E. Calvet, P. Bessière, J. Droulez, and D. Querlioz, "Bayesian inference with Müller C-elements," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 63, no. 6, pp. 895–904, Jun. 2016, doi: 10.1109/TCSI.2016.2546064.

[6] P. A. Merolla, J. V. Arthur, R. Alvarez-Icaza, A. S. Cassidy, J. Sawada, F. Akopyan, B. L. Jackson, N. Imam, C. Guo, and Y. Nakamura, "A million spiking-neuron integrated circuit with a scalable communication network and interface," *Science*, vol. 345, no. 6197, pp. 668–673, Aug. 2014, doi: 10.1126/science.1254642.

[7] G. Pedretti, V. Milo, S. Ambrogio, R. Carboni, S. Bianchi, A. Calderoni, N. Ramaswamy, A. S. Spinelli, and D. Ielmini, "Stochastic learning in neuromorphic hardware via spike timing dependent plasticity with RRAM synapses," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 8, no. 1, pp. 77–85, Mar. 2018, doi: 10.1109/JETCAS.2017.2773124.

[8] D. Vodenicarevic, N. Locatelli, A. Mizrahi, J. S. Friedman, A. F. Vincent, M. Romera, A. Fukushima, K. Yakushiji, H. Kubota, and S. Yuasa, "Low-energy truly random number generation with superparamagnetic tunnel junctions for unconventional computing," *Phys. Rev. Appl.*, vol. 8, no. 5, p. 054045, Nov. 2017, doi: 10.1103/PhysRevApplied.8.054045.

[9] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006, doi: 10.1142/S0218127406015970.

[10] J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Cryptanalytic attacks on pseudorandom number generators," in *Fast Software Encryption*. Berlin, Germany: Springer, Oct. 1998, pp. 168–188, doi: 10.1007/3-540-69710-1-12.

[11] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, p. 145, Mar. 2002, doi: 10.1103/RevModPhys.74.145.

[12] B. Jun and P. Kocher, "The Intel random number generator," Cryptogr. Res., Inc., San Francisco, CA, USA, White Paper, Apr. 1999.

[13] S. Sahay and M. Suri, "Recent trends in hardware security exploiting hybrid CMOS-resistive memory circuits," *Semicond. Sci. Technol.*, vol. 32, no. 12, p. 123001, Oct. 2017, doi: 10.1088/1361-6641/aa8f07.

[14] R. Brederlow, R. Prakash, C. Paulus, and R. Thewes, "A low-power true random number generator using random telegraph noise of single oxide-traps," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2006, pp. 1666–1675, doi: 10.1109/ISSCC.2006.1696222.

[15] C.-Y. Huang, W. C. Shen, Y.-H. Tseng, Y.-C. King, and C.-J. Lin, "A contact-resistive random-access-memory-based true random number generator," *IEEE Electron Device Lett.*, vol. 33, no. 8, pp. 1108–1110, Aug. 2012, doi: 10.1109/LED.2012.2199734.

[16] A. Fukushima, T. Seki, K. Yakushiji, H. Kubota, H. Imamura, S. Yuasa, and K. Ando, "Spin dice: A scalable truly random number generator based on spintronics," *Appl. Phys. Exp.*, vol. 7, no. 8, p. 083001, Jul. 2014, doi: 10.7567/APEX.7.083001.

[17] S. Chun, S.-B. Lee, M. Hara, W. Park, and S.-J. Kim, "High-density physical random number generator using spin signals in multidomain ferromagnetic layer," *Adv. Condens. Matter Phys.*, vol. 2015, Jan. 2015, Art. no. 251819, doi: 10.1155/2015/251819.

[18] Z. Wei, Y. Katoh, S. Ogasahara, Y. Yoshimoto, K. Kawai, Y. Ikeda, K. Eriguchi, K. Ohmori, and S. Yoneda, "True random number generator using current difference based on a fractional stochastic model in 40-nm embedded ReRAM," in *IEDM Tech. Dig.*, Dec. 2016, pp. 4.8.1–4.8.4, doi: 10.1038/s41467-017-00869-x.

[19] 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.

[20] S. Balatti, S. Ambrogio, R. Carboni, V. Milo, Z. Wang, A. Calderoni, N. Ramaswamy, and D. Ielmini, "Physical unbiased generation of random numbers with coupled resistive switching devices," *IEEE Trans. Electron Devices*, vol. 63, no. 5, pp. 2029–2035, May 2016, doi: 10.1109/TED.2016.2537792.

[21] A. F. Vincent, N. Locatelli, J. O. Klein, W. S. Zhao, S. Galdin-Retailleau, and D. Querlioz, "Analytical macrospin modeling of the stochastic switching time of spin-transfer torque devices," *IEEE Trans. Electron Devices*, vol. 62, no. 1, pp. 164–170, Jan. 2015, doi: 10.1109/TED.2014.2372475.

[22] S. Ambrogio, S. Balatti, A. Cubeta, A. Calderoni, N. Ramaswamy, and D. Ielmini, "Statistical fluctuations in $HfO_x$ resistive-switching memory: Part I—Set/reset variability," *IEEE Trans. Electron Devices*, vol. 61, no. 8, pp. 2912–2919, Aug. 2014, doi: 10.1109/TED.2014.2330200.

[23] 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.

[24] Y. Qu, J. Han, B. F. Cockburn, W. Pedrycz, Y. Zhang, and W. Zhao, "A true random number generator based on parallel STT-MTJs," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Mar. 2017, pp. 606–609, doi: 10.23919/DATE.2017.7927058.

[25] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST, Gaithersburg, MD, USA, Tech. Rep. SP 800-22, Sep. 2001.

[26] R. Carboni, S. Ambrogio, W. Chen, M. Siddik, J. Harms, A. Lyle, W. Kula, G. Sandhu, and D. Ielmini, "Understanding cycling endurance in perpendicular spin-transfer torque (p-STT) magnetic memory," in *IEDM Tech. Dig.*, Dec. 2016, pp. 21.6.1–21.6.4, doi: 10.1109/IEDM.2016.7838468.

[27] D. Apalkov, B. Dieny, and J. Slaughter, "Magnetoresistive random access memory," *Proc. IEEE*, vol. 104, no. 10, pp. 1796–1830, Oct. 2016, doi: 10.1109/JPROC.2016.2590142.

[28] Z. Li and S. Zhang, "Thermally assisted magnetization reversal in the presence of a spin-transfer torque," *Phys. Rev. B, Condens. Matter*, vol. 69, no. 13, p. 134416, 2004, doi: 10.1103/PhysRevB.69.134416.

[29] G. Jan, L. Thomas, S. Le, Y.-J. Lee, H. Liu, J. Zhu, J. Iwata-Harms, S. Patel, R.-Y. Tong, and S. Serrano-Guisan, "Achieving sub-ns switching of STT-MRAM for future embedded LLC applications through improvement of nucleation and propagation switching mechanisms," in *IEEE Symp. VLSI Technol. Dig. Tech. Papers*, Jun. 2016, pp. 1–2, doi: 10.1109/VLSIT.2016.7573362.

[30] R. Heindl, W. H. Rippard, S. E. Russek, M. R. Pufall, and A. B. Kos, "Validity of the thermal activation model for spin-transfer torque switching in magnetic tunnel junctions," *J. Appl. Phys.*, vol. 109, no. 7, p. 073910, 2011. [Online]. Available: http://dx.doi.org/10.1063/1.3562136, doi: 10.1063/1.3562136.

[31] C. Cagli, F. Nardi, and D. Ielmini, "Modeling of set/reset operations in NiO-based resistive-switching memory devices," *IEEE Trans. Electron Devices*, vol. 56, no. 8, pp. 1712–1720, Aug. 2009, doi: 10.1109/TED.2009.2024046.