Spin Dice Based on Orthogonal Spin-Transfer Devices With Planar Polarizer

Xin Li, Shijiang Luo, Hanzhang Qin, Jeongmin Hong, and Long You

School of Optical and Electronic Information, Huazhong University of Science and Technology, Wuhan 430074, China

Multi-junctional magnetic tunneling junction spin dice based on orthogonal spin-transfer devices, a new type of true random number (RN) generator (TRNG) is demonstrated in this paper. Orthogonal spin-transfer devices use a planar polarizer to push the free layer with perpendicular anisotropy to metastable state (high-energy state) when power is on. The stochastic precessional switching behavior in ferromagnetic free layer is utilized as the entropy source of the TRNG. Once the power is turned off, anisotropy field and demagnetization field relax the magnetization of free layer from metastable state to one of the two stable states, producing a random bit whose value is solely determined by the stochastic switching behavior. The generation and detection of random bits were summarized under the macrospin picture. RN sequences with high randomness can be produced steadily in the proposed TRNG with a wide operation range of temperature and applied current density. Furthermore, the RN sequences pass the statistical test of NIST SP-800 with an appropriate pass rate without any need of post-procession of data. Ease of design, ultrafast switching as well as high randomness of the bit sequences make the proposed TRNG a competitive device in information security field.

Index Terms—**Magnetic tunneling junction (MTJ), orthogonal, planar polarizer, spin transfer, true random number generator (TRNG).**

I. Introduction

WITH the advent of the era of big data, informatization brings convenience to daily life, at the same time, the problem of information security becomes increasingly prominent. True random number (RN) generator (TRNG), based on physical entropy sources [1]–[4], acts a crucial role in cryptography and information security applications [5]–[7]. Practical RNs generating methods are the research emphasis in cryptographic algorithm, which leads much efforts paid on the design of TRNG. However, almost all the conventional TRNGs [4], [8] have the shortcomings of significantly high-power consumption, poor scalability, and very narrow operation region on temperature. The spintronics-based TRNG, referred to as "spin dice" [9], uses the inherent thermal noise presented in the device as the entropy source. Usually, two current pulses are needed in the spin dice; namely, the "reset" pulse to initialize the magnet to a stable state and subsequently the "roll" pulse to orient the magnet to a high-energy state and then rotate it with a probability of 50%. Unfortunately, under the aforementioned switching mechanism, the switching probability of 50% only occurs in very narrow ranges of input current density and external temperature.

In this paper, we propose this two-terminal spin dice based on orthogonal spin-transfer devices. Three magnetization layers are constructed in the orthogonal magnetic tunneling junction (MTJ), where the free layer and polarizer work together to complete the reset" and "roll" process; the free layer and analyzer work together to complete the "read" process. The chaotic switching behavior motivated by spin-transfer torque (STT) in the nanomagnet is utilized as the entropy source to produce a random magnetization. Initialization is completed in the "reset" process. In the "roll" process, magnetization of the free layer was pulled to the metastable state and then fell to one of the stable states, a random bit is generated and subsequently detected, thus make one period come to an end. Furthermore, RN sequences produced by the proposed TRNG could embody extremely high quality accompanied with high reliability and efficiency without any post-procession [9], [10] (e.g., XOR operation). Besides, the proposed TRNG could still work effectively even when the external conditions including the temperature and applied current density changed sharply; therefore, the operation region could be expanded. With the simulation results provided, we argue that the proposed TRNG could overcome the earlier described problems including poor scalability and narrow operation region; we argue that the multi-junctional spin dice is a promising candidate for scalable truly RN generator which is suitable for encrypting.

Manuscript received March 14, 2018; revised April 15, 2018; accepted April 24, 2018. Date of publication June 12, 2018; date of current version October 17, 2018. Corresponding author: L. You (e-mail: lyou@hust.edu.cn).

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

Digital Object Identifier 10.1109/TMAG.2018.2832194

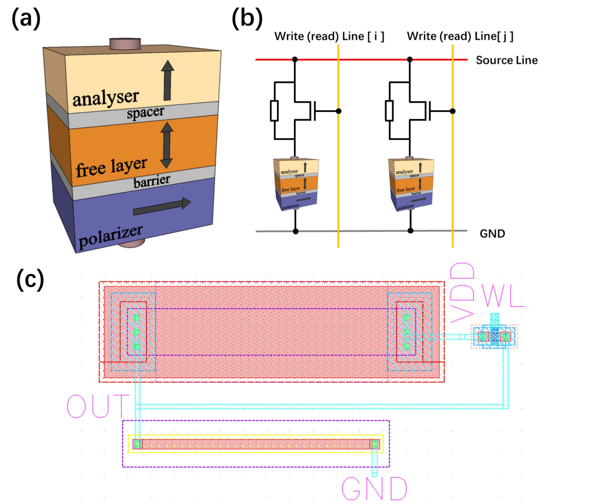

Fig. 1. (a) Structure of the TRNG with planar polarizer and perpendicular free layer. (b) Sampling circuit of the TRNG. (c) Corresponding circuit layout of the sampling circuit in (b).

II. Device Design and Macrospin Modeling

The device structure of the proposed TRNG is illustrated in Fig. 1(a). A MgO barrier is sandwiched between the polarizer and free layer, while a nonmagnetic spacer is caught in the middle of the analyzer and free layer. Easy magnetic axis direction of the analyzer and free layer is parallel but magnetic anisotropy direction of polarizer and the other two layers are orthogonal. Both of the structures can work successfully under nearly the same mechanism whether the TRNG has a planar free layer [11], [12] or a perpendicular free layer [13], [14], as shown in Fig. 1(a). However, the latter one has much better thermal stability and scalability, also smaller critical current density [15]. In this paper, all the simulations and tests are completed based on the structure with a planar polarizer and a perpendicular free layer. The free layer is designed to have a much smaller anisotropy field than that of the other two ferromagnetic layers to assure that under the given applied current density, magnetization switching only happens in the free layer. This can be achieved by setting pinned layers under the planar polarizer and upon the perpendicular analyzer to fix their magnetization direction. Switchable free layer along with invariable analyzer and polarizer could make the "reset" and "roll" procedures operate well.

A. Implementation and Operation

The proposed TRNG is a two-terminal device. Two current pulses through the same access are required to generate RNs. One of the pulses is needed in the process of "roll" to generate a random bit and the other one is needed in the "read" process to detect the random bit. The "reset" MTJ, including the polarizer and free layer, is used to reset the TRNG, namely, initialize the magnetization of free layer to a stable state. The "roll" pulse is utilized to supply a strong enough spin torque to rotate the magnetization of free layer parallel or anti-parallel with the spin polarized direction according to electron flows direction, which is orthogonal to the magnetic anisotropy direction of free layer. Therefore, magnetization of free layer stays in metastable state. After that the "roll" pulse is turned off, without support of spin torque, magnetic anisotropy field and demagnetization field relax magnetization of the free layer. Finally, it goes back to easy magnetic axis direction, namely, one of the two stable states. The initial states for analyzer and free layer, parallel, or anti-parallel, have no influence on the switching probability in the rolling process.

Precessional switching is excited when the polarizer and free layer have orthogonal magnetization. During the stochastic precessional switching process [16], magnetization of free layer is assisted out of plane with help of the strong spin torque, leading to a high-energy state in the energy landscape of the nanomagnet. With equivalent attractions of the two stable states, orientation of free layer presents unpredictable, resulting in a probabilistic switching at the moment the "roll" pulse turned off. Also, inherent thermal noise presented in the device has a contribution to the chaos of the switching process. As the amplitude of thermal fluctuation field and magnetization direction are both nondeterministic, the precessional switching is inherently more chaotic.

The "read" MTJ including analyzer and free layer is utilized to detect the impedance state of the MTJ stack. "Read" pulse, which do not supply a large enough spin torque to switch the free layer nanomagnet, is applied on the TRNG stack to detect its resistance state. Low-resistance state could be detected when the random state of free layer and the magnetization direction of analyzer are parallel (corresponding to random bit "0"), otherwise, high-resistance state can be detected when the magnetization directions are anti-parallel (corresponding to random bit "1").

One period including generation of a random bit and detection of its value is implemented with the operation of applying a "roll" pulse and a "read" pulse on the TRNG. Random bits are produced by the sampling circuit, as shown in Fig. 1(b), and accompanied with the circuit layout, as depicted in Fig. 1(c). Current pulses diagram in one period and the corresponding magnetization state of the free layer are shown in Fig. 2(a). Source and write enable signals pass through the TRNG stack in the same access. In the read process, a fixed resistor is placed here to limit the read current, which should be smaller than the critical switching current of the nanomagnet. In the same device but at different runs, the magnetization dynamics of the free layer in the z-axis direction is shown in Fig. 2(b).

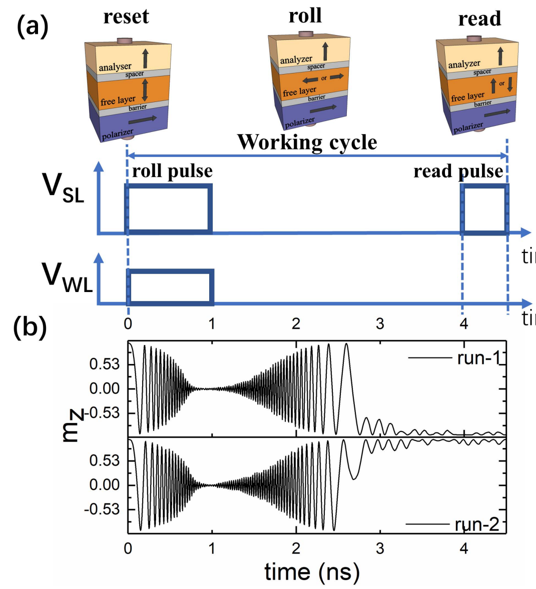

Fig. 2. (a) Current pulses diagram in one period and the corresponding magnetization state of the proposed TRNG. (b) Magnetization dynamics of the free layer in the z-axis direction in different runs.

B. Numerical Simulations

STT effect is the pivotal mechanism in controlling the magnetization state of free layer nanomagnet and the resistance state of the stack in the proposed TRNG device. The time-dependent evolution of the magnetization in free layer, affected by the spin torques both from the analyzer and polarizer, can be obtained by solving the Landau-Lifshitz-Gilbert (LLG) equation with the Slonczewski term [17], namely the LLGS equation mathematically given as

$$\frac{d\vec{M}}{dt} = -\gamma\mu_0(\vec{M}\times\vec{H_{\text{eff}}}) + \frac{\alpha}{M_s}\left(\vec{M}\times\frac{d\vec{M}}{dt}\right) - \frac{\gamma\cdot\hbar\cdot J}{M_S^2\cdot d\cdot e}\{g_1(\theta_1)[\vec{M}\times(\vec{M}\times\vec{\sigma_1})] + g_2(\theta_2)[\vec{M}\times(\vec{M}\times\vec{\sigma_2})]\}. \quad (1)$$

Key terms of LLGS equation are shown in (1). $\vec{H_{\text{eff}}}$ refers to the effective magnetic field, including uniaxial anisotropy field, demagnetization field, *Zeeman* effects, and thermal fluctuation-induced field. The thermal fluctuation-induced field could be calculated as

$$H_{fl} = \sqrt{2\alpha k_B T/\gamma\mu_0 V M_s d} \quad (2)$$

where γ, μ_0, e, $\hbar$, k_B, and T are the gyromagnetic ratio of the electrons, the vacuum permeability, the elementary charge, reductive *Planck* constant, Boltzmann's constant, and environmental temperature, respectively; V, d, and α are the volume, thickness, and *Gilbert* damping factor of the material of free layer, respectively; J is the current density applied on the TRNG stack; g_1 and g_2 are the efficiency factor of the STT on the polarizer and analyzer, respectively, which has a dependence on p_1/p_2, the spin polarization value of polarizer and analyzer, respectively, and θ_1 and θ_2 are the angles between the magnetization direction of free layer and analyzer/polarizer layer. The efficiency factor of STT on polarizer can be calculated as

$$g_1 = \left[-4 + (1+p_1)^3(3+\cos\theta_1)\big/\left(4p_1^{3/2}\right)\right]^{-1}. \quad (3)$$

The factor on analyzer could also be calculated in similar way. p_1 and p_2 are setting as 0.6 and 0.1, respectively, in the proposed structure; $\overrightarrow{\sigma_1}$ and $\overrightarrow{\sigma_2}$ are unit vector for magnetization of the polarizer and analyzer, respectively.

Magnetization procession of the free layer nanomagnet as well as the detection of RN sequences is simulated. These conditions can be summarized under the macrospin picture based on LLGS equation. Size of the free layer nanomagnet is 50 nm × 50 nm × 2 nm, which can be treated as a single magnetic domain nanomagnets. The saturation magnetization (M_s), magnetic anisotropy energy density (K_u), and *Gilbert* damping constant (α) are 1000 emu/cc, 0.7×10^7 erg/cc, and 0.014, respectively, for the free layer with perpendicular anisotropy, which is consistent with CoFeB-based FM material properties [10].

Throughput of the TRNG per device not only depends on "reset" and "roll" time but also on "relax" and "read" time durations. Considering "roll" pulse duration as 1 ns and "relax" process duration as 3 ns, one total period of the TRNG is evaluated to be 4.8 ns with addition of "read" process (0.5 ns) and "reset" process (0.3 ns) in approximately. The proposed TRNG with a planar polarizer has a bit rate of 208 Mb/s (at 300 K), which is much higher than those of the existing RNGs [18]–[20].

III. Results and Discussion

A. Operation Region

In the nanomagnets that based on the damping mechanism, a switching probability of 50% only occurs in a very narrow and strict region. Robust operation of digital microprocessor in a dynamic voltage scaling environment is extremely challenging. Unlike that, we highlight the fact that operation of the proposed device is insensitive to variations around the process conditions due to the independent entropy source of thermal fluctuations. Analysis was performed for bit streams generated under different current densities and temperatures in a range to evaluate the performance of our TRNG. As shown in Fig. 3(a), in the case that current density varies from 7.80 × 10^7–8.20 × 10^7 A/cm^2 and the environment temperature varies from 200–400 K, the switching probability floats around 0.5 with tiny fluctuations. Each numerical value of switching probability ($P_{\rm sw}$) is obtained from 100 000 random bits and it represents the proportion of "1" in total random bits. The percentage in vertical coordinates of the graphs shown in Fig. 3 is relative error, which is equal to $[(P_{\rm sw} - 0.5)/0.5] \times 100\%$. It is not hard to find that the relative error of $P_{\rm sw}$ is less than 1%. Thermal stability and tolerability of imperfections in materials possessed by the proposed TRNG make it a competitive device in extreme conditions. Furthermore, unstable voltage supply could hardly have any influence on the performance of the proposed device. Therefore, the robustness of the TRNG device [21] can maintain over process and temperature variations.

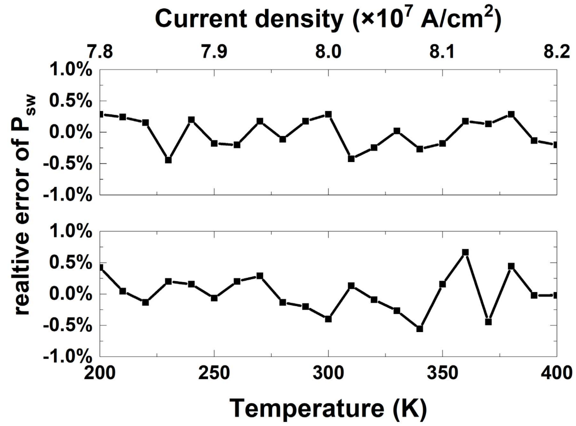

Fig. 3. Relative error of switching probability for bit streams generated under different current densities and temperatures.

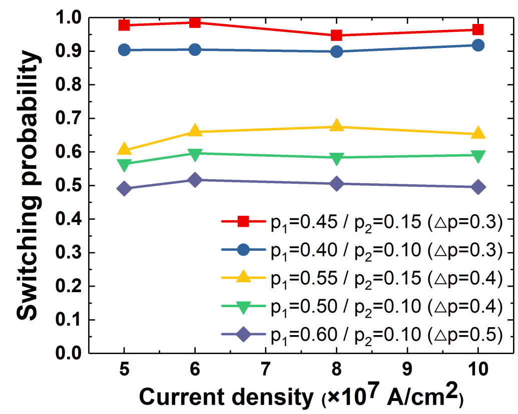

Fig. 4. Switching probability for bit streams generated under different spin polarization values of the analyzer and polarizer.

B. Switching Probability Versus Spin Polarization

Magnetization switching does not happen in analyzer and polarizer. Both of them have contributions of transferring the spin torque to free layer through tunneling barrier or the nonmagnetic spacer due to the STT effect in the proposed structure. The spin polarization of analyzer is designed to be far less than that of polarizer to ensure that the spin torque from the analyzer is not sufficient to influence the randomness of RN sequences. Without the analyzer, magnetization of free layer can stay firmly in the high-energy state and relax down with a probability of 50% exactly because the only spin torque is polarized perpendicular to the easy axis direction of free layer. Existence of analyzer in one way makes reading of the random bit more convenient but unfortunately has a negative effect on the precession of the nanomagnet due to the collinear easy magnetic axis with the analyzer. In this way, it is essential to regulate the spin polarization value of analyzer and polarizer to ensure the randomness of the RN sequences.

In Fig. 4, we make a thorough inquiry about the relationship between the spin polarization gap of the analyzer and polarizer under different applied current densities. The results indicate that a disparity of the spin polarization between analyzer and polarizer is required to get RN sequences with high randomness. According to the LLGS equation which has been mentioned earlier, the polarized direction of the analyzer has a contribution to the precessional switching of the free layer which is correlate with the spin polarization value.

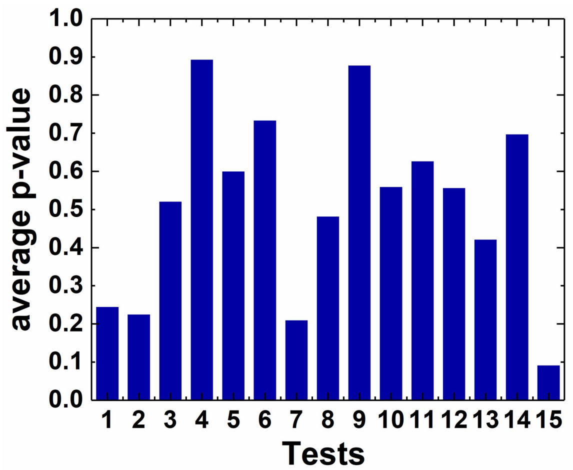

Fig. 5. NIST test results for the TRNG at 300 K. The RN sequence is generated by the TRNG with planar polarizer. The individual tests are: (1) approximate entropy, (2) block frequency, (3) cumulative sums, (4) discrete Fourier transform, (5) frequency, (6) linear complexity, (7) longest runs, (8) nonoverlapping template, (9) overlapping template, (10) random excursions, (11) random excursion variant, (12) rank, (13) runs, (14) serial, and (15) Maurer's universal.

In addition, randomness of RN sequences under all cases of spin polarization is almost uncorrelated with current density within limits.

C. NIST Test of Randomness

NIST's SP 800-22 statistical test [22] was utilized to test the randomness of the generated bit streams which have not been treated with any post-processions. A million bits of RNs were generated in the proposed structure. Testing results of the RN sequences are shown in Fig. 5. This test suite consists of 15 kinds of statistical tests (188 tests in all). It should be noted that these statistical tests are not simple yes–no tests but significance tests with a certain pass rate. Tests are considered passing when p-value >0.01. For the tests which produce multiple p-values and individually all of them were above 0.01, the histogram shown in Fig. 5 only shows the average p-value for the sake of simplicity. It is not hard to find that the RN sequence passed all the 15 NIST Special Publication 800-22 randomness tests without any post-processing of data, such as XOR operation. Test results of our TRNG confirm its reliable performance.

IV. Conclusion

We have proposed a TRNG based on orthogonal spin-transfer MTJ construction. The TRNG works in very straightforward circuit with stochastic precessional switching behavior as the entropy source and produces RN sequences with strong randomness. RN generation in the proposed TRNG only requires the application of "reset" and "roll" voltage pulses. Besides, our TRNG is very robust and reliable. It can operate in a wide range of temperature and current density without any distortions in the entropy. Large gap of spin polarization value between the analyzer and the polarizer is required to ensure the quality of the TRNG. It also combines fast switching and wide operation window, both of which are critical for applications. RN sequences generated from the proposed TRNG could pass through the NIST test without any XOR operation. With the simulation results demonstrated earlier, the proposed device is proven to be a reliable and promising TRNG with high performance.

Acknowledgment

This work was supported by the National Natural Science Foundation of China under Grant 61674062.

References

[1] C. Gabriel *et al.*, "A generator for unique quantum random numbers based on vacuum states," *Nature Photon.*, vol. 4, no. 10, pp. 711–715, Oct. 2010.

[2] M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro, "Secure self-calibrating quantum random-bit generator," *Phys. Rev. A, Gen. Phys.*, vol. 75, no. 3, pp. 032334-1–032334-6, Mar. 2007.

[3] P. J. Bustard, D. Moffatt, R. Lausten, G. Wu, I. A. Walmsley, and B. J. Sussman, "Quantum random bit generation using stimulated Raman scattering," *Opt. Exp.*, vol. 19, no. 25, pp. 25173–25180, 2011.

[4] A. Uchida *et al.*, "Fast physical random bit generation with chaotic semiconductor lasers," *Nature Photon.*, vol. 2, no. 12, pp. 728–732, 2008.

[5] S. Yuasa *et al.*, "Future prospects of MRAM technologies," in *IEDM Tech. Dig.*, Dec. 2013, pp. 3.1.1–3.1.4.

[6] K. Yang, D. Fick, M. B. Henry, Y. Lee, D. Blaauw, and D. Sylvester, "A 23 Mb/s 23 pJ/b fully synthesized true-random-number generator in 28 nm and 65 nm CMOS," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2014, pp. 280–281.

[7] M. Stipčević and C. K. Koç, "True random number generators," in *Open Problems in Mathematics and Computational Science*. Cham, Switzerland: Springer, 2014, pp. 275–315.

[8] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, "Ultrahigh-speed random number generation based on a chaotic semiconductor laser," *Phys. Rev. Lett.*, vol. 103, no. 2, pp. 024102-1–024102-4, Jul. 2009.

[9] A. Fukushima *et al.*, "Spin dice: A scalable truly random number generator based on spintronics," *Appl. Phys. Exp.*, vol. 7, no. 8, p. 083001, 2014.

[10] N. Rangarajan, A. Parthasarathy, and S. Rakheja, "A spin-based true random number generator exploiting the stochastic precessional switching of nanomagnets," *J. Appl. Phys.*, vol. 121, p. 223905, Jun. 2017.

[11] D. Houssameddine *et al.*, "Spin-torque oscillator using a perpendicular polarizer and a planar free layer," *Nature Mater.*, vol. 6, no. 6, pp. 447–453, 2007.

[12] U. Ebels *et al.*, "Macrospin description of the perpendicular polarizer-planar free-layer spin-torque oscillator," *Phys. Rev. B, Condens. Matter*, vol. 78, p. 024436, Jul. 2008.

[13] R. Lehndorff *et al.*, "Magnetization dynamics in spin torque nano-oscillators: Vortex state versus uniform state," *Phys. Rev. B, Condens. Matter*, vol. 80, p. 054412, Aug. 2009.

[14] Z. Zeng, G. Finocchio, and H. Jiang, "Spin transfer nano-oscillators," *Nanoscale*, vol. 5, no. 6, pp. 2219–2231, 2013.

[15] R. Law, E.-L. Tan, R. Sbiaa, T. Liew, and T. C. Chong, "Reduction in critical current for spin transfer switching in perpendicular anisotropy spin valves using an in-plane spin polarizer," *Appl. Phys. Lett.*, vol. 94, no. 6, p. 062516, 2009.

[16] A. V. Khvalkovskiy, J. Grollier, N. Locatelli, Y. V. Gorbunov, K. A. Zvezdin, and V. Cros, "Nonuniformity of a planar polarizer for spin-transfer-induced vortex oscillations at zero field," *Appl. Phys. Lett.*, vol. 96, no. 21, p. 212507, 2010.

[17] J. C. Slonczewski, "Current-driven excitation of magnetic multilayers," *J. Magn. Magn. Mater.*, vol. 159, pp. L1–L7, Jun. 1996.

[18] 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.

[19] A. Rukhin *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST Special Pub. 800-822, 2010.

[20] M. Barangi, J. S. Chang, and P. Mazumder, "Straintronics-based true random number generator for high-speed and energy-limited applications," *IEEE Trans. Magn.*, vol. 52, no. 1, Jan. 2016, Art. no. 3400109.

[21] S. Srinivasan *et al.*, "2.4 GHz 7 mW all-digital PVT-variation tolerant true random number generator in 45 nm CMOS," in *Proc. IEEE Symp. VSLI Circuits*, Jun. 2010, pp. 203–204.

[22] W. H. Choi *et al.*, "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. 121–125.