Straintronics-Based True Random Number Generator for High-Speed and Energy-Limited Applications

Mahmood Barangi[1], Joseph S. Chang[2], and Pinaki Mazumder[1], *Fellow, IEEE*

[1]Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI 48109-2122 USA
[2]Department of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798

Random number generators are well known for their ubiquitous use in cryptography, statistical sampling, and computer simulations. In order to establish secure data transfers in cryptographic applications, these number generators need to reliably produce unpredictable numbers at a high rate. In this paper, by exploiting the metastability of the stressed straintronics (STR) device, we theoretically propose a proof-of-concept nanomagnetic-based scheme to generate random numbers at very high rates with low-energy overhead. The dynamic modeling of the device, including the Langevin thermal noise field, is discussed, and the effect of process variation on the energy barrier and reliability is analyzed. The device is interfaced with CMOS circuitry and simulated in the 65 nm technology. At 1 V supply level, the system can generate random numbers as fast as 510 MHz. The entire circuit, including the CMOS peripherals, consumes 12.5 uW at 100 MHz random number generation rate while dissipating merely 0.125 pJ/bit. By reducing the supply level to 0.5 V, the energy per bit can be reduced further to 19 fJ. Since the STR device can be placed on the top of the CMOS circuitry, the total area of the design is estimated to be 0.001 mm^2.

Index Terms— **Energy barrier, entropy, magnetic tunneling junction (MTJ), magnetization, magnetostriction, metastability, piezoelectricity, random number generator (RNG), strain, straintronics (STR), stress, Villari effect.**

I. Introduction

THE concept of random number generation is easily understood from early childhood when we look into our experience of rolling a die, flipping a coin, or playing cards. As a matter of fact, if the coin or the die is flawless, a truly random outcome is expected. This is associated with the idea of a true random number generator (TRNG). Physical damage to the coin or the die can make the results more predictable, leading to a less reliable RNG. In communication and cryptography, a predictable RNG will expose sensitive data to the possible attackers. While the randomness of the output is the most important quality of an RNG, in real systems, other qualities are also of crucial importance. For example, if an RNG consumes a significant amount of energy, takes up a large area, or operates at very low speeds in order to achieve high randomness, it will not be practical in many applications. The lack of speed in random number generation can cause performance issues in Web and mail servers [1]. As a result, a design for high-speed, area-efficient, and low-power TRNG has been a focus of both the software and the hardware research for decades.

RNGs can be implemented using software algorithms [2]–[4]. While these algorithms usually produce pseudorandom numbers with many fewer design complications than hardware-based RNGs, they employ a general processor for their operation. This makes these software-based approaches power-hungry and area-inefficient. In addition, since a general processor is not specifically designed for the purpose of random number generation, it will be generating random numbers at much lower speeds than the RNG hardware.

Integrated circuits (ICs) are widely used to implement the RNGs in the hardware. A variety of application-specific ICs are solely designed for the purpose of true random number generation [6]–[16] or pseudorandom number generation [17], [18]. They provide random numbers at much higher speeds, with much lower power and area overhead compared with their software-based peers. TRNG ICs use two popular approaches in order to generate random data: 1) a metastable structure with a high gain can be used in order to amplify small noise into random digital binary data [6], [7]. This is shown in Fig. 1(a), where a back-to-back inverter is reset into a metastable state. Then, in the next cycle, the RST signal is removed and the evaluation occurs. Due to the high gain of the back-to-back loop, one side randomly settles at logic one, while the other side settles at logic zero. However, due to mismatch and process variation, a single back-to-back loop will almost never generate a truly random number; therefore, calibration is required. Different approaches are proposed for the calibration. Mathew *et al.* [6] use a digital calibration scheme with delay elements and the inverter's pull-up and pull-down adjustments in order to achieve randomness, as shown in Fig. 1(b). Another approach is to use a feedback loop and inject charges to one side of the back-to-back loop in order to balance out the mismatch effect [7], which is also shown in Fig. 1(b). Both of these approaches, however, invest a significant amount of energy on calibration circuitry, and the core RNG (the back-to-back loop) ends up consuming a small portion of the total energy and 2) a high-frequency clock can be combined with a low-frequency jittery clock to generate a random sequence, as shown in Fig. 1(c). The slow and fast clock generators usually consume a great deal of power and occupy a large area on the chip. Bucci *et al.* [8] use this approach,

Manuscript received June 9, 2015; revised July 27, 2015; accepted September 2, 2015. Date of publication September 14, 2015; date of current version December 18, 2015. Corresponding author: M. Barangi (e-mail: barangi@umich.edu).

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.2015.2478398

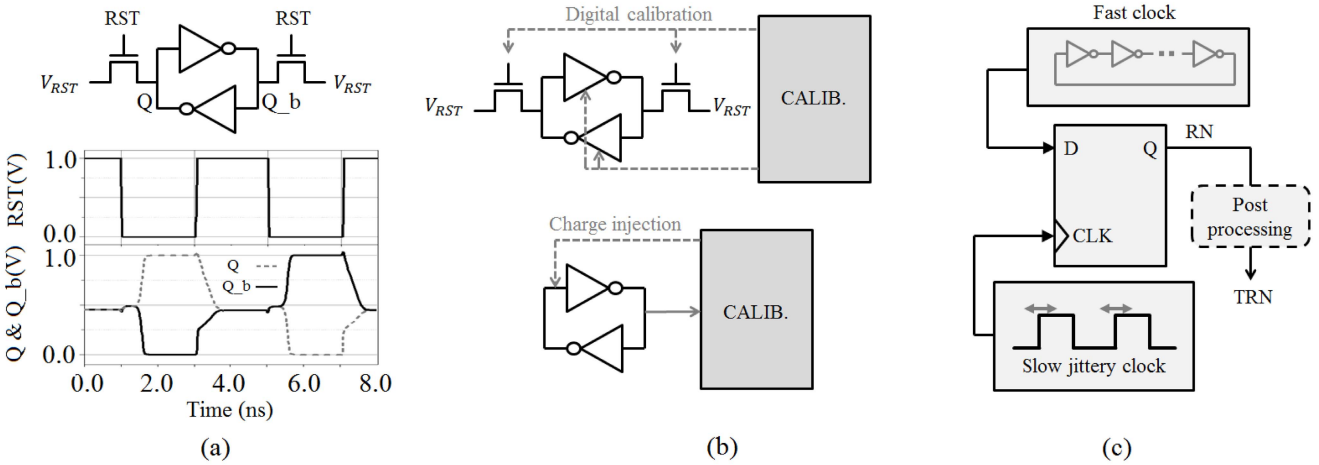

Fig. 1. (a) Taking the advantage of the metastability of the back-to-back inverter loop to generate the random data. (b) Calibration of the back-to-back inverter loop using a controller circuitry or charge injection. (c) Use of fast clock and slow jittery clock to generate random numbers.

which consumes 0.23 nJ for each generated random bit. Petrie and Connelly [9] combine 1) and 2) with discrete-time, chaos-based systems in order to achieve a better randomness. However, this makes the system area and energy inefficient, leading to 1.5 mm^2 area and 3.9 nJ/bit energy consumption.

The use of nanomagnets in logic and memory design has drawn much attention in research laboratories in the past decades [19]–[22]. These designs exploit the principle of tunnel magnetoresistance (TMR) in order to store a logic value into a magnetic tunneling junction (MTJ). MTJ consists of two magnetic layers separated by a tunneling barrier. The resistance of the MTJ can vary between high and low values based on the relative orientation of the magnetization vectors in the two magnetic layers. The conventional MTJ-based designs switch between high and low states with no metastable state in between. Therefore, they cannot be viable candidates for the TRNG design. Recently, the concept of straintronics has been proposed as an energy efficient means to switch the state of a magnetic layer using the piezoelectricity and Villari effect (inverse magnetostriction) [23]–[27]. Practical demonstration of the straintronics principle is under investigation, and successful switching of the magnetization has been demonstrated recently [28]–[30]. The principle of the straintronics states that in the presence of physical stress, the Straintronics MTJ will settle into a metastable point, and upon removal of stress, it relaxes back at high- or low-resistance states. While this metastability can add to design complexities in the straintronics memory and logic [25], it can be handy in the design of TRNGs.

In this paper, we exploit the metastable state of the straintronics MTJ [25], [27] in order to build a TRNG. Modeling of thermal noise and the effect of process variation are analyzed. We interface our straintronics device (STR) with the CMOS circuitry and simulate the system for power, speed, and unpredictability metrics. The rest of this paper is organized as follows. Section II describes the straintronics principle and the methodology that we used for the TRNG design based on this principle. Section III describes the modeling of the dynamic behavior, the effect of thermal noise and process variation, and the choice of material for the free layer of MTJ.

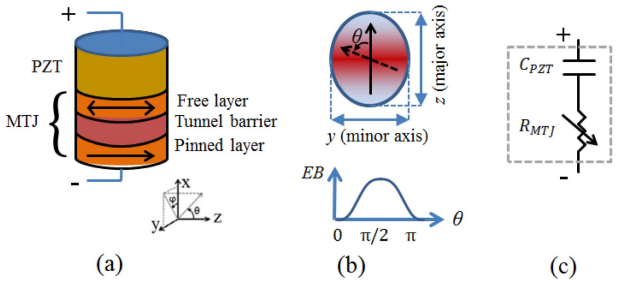

Fig. 2. (a) Straintronics device. (b) Demonstration of the major and minor axes and the magnetic energy barrier. (c) Equivalent RC model.

Section IV is dedicated to the cell design. The simulation results are highlighted in Section V. Finally, the conclusion is drawn in Section VI.

II. Proposal of TRNG Using the Straintronics Principle

Fig. 2(a) shows the view of the STR. The device is made by placing a piezoelectric layer (PZT) on the top of an MTJ. The MTJ consists of two nanomagnets, separated by a tunneling barrier. The pinned layer has a fixed magnetic orientation along the $+z$-axis. The magnetic orientation of the free layer can switch between the $+z$-axis (parallel to the pinned layer, where $\theta = 0$) and the $-z$-axis (antiparallel to the pinned layer, where $\theta = \pi$). The free layer is a magnetostrictive material. The device takes the advantage of piezoelectricity and inverse magnetostriction in order to assist flipping of the magnetization state. The device is a cylindrical ellipse with the minor and major axes placed on the y–z plane, as shown in Fig. 2(b). The major axis and minor axis dimensions are chosen to be $a = 110$ nm and $b = 90$ nm, respectively, providing reliability against process variations (discussed in Section III). The thickness ratio of the PZT to the free layer is chosen to be 40/10 nm in order to provide a large plane interface between the layers to assure perfect transfer of a strain [23], [24]. In the absence of external forces, the free layer settles along the major axis due to the magnetic and shape anisotropies of the free layer [31]. These anisotropies

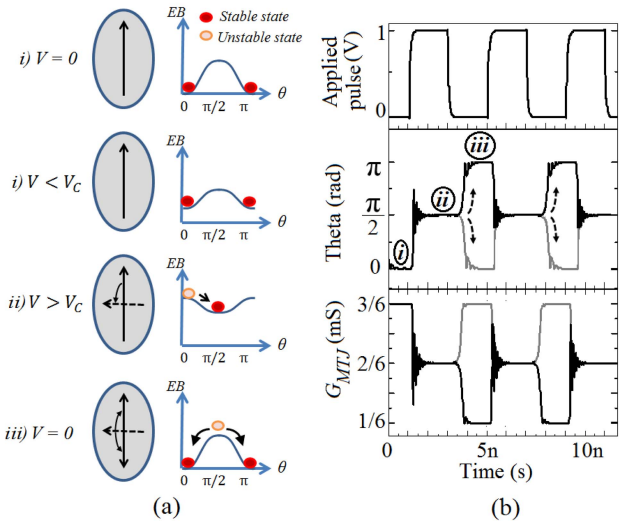

Fig. 3. Demonstration of the random final state of the STR using (a) energy barrier plots and (b) dynamic waveforms.

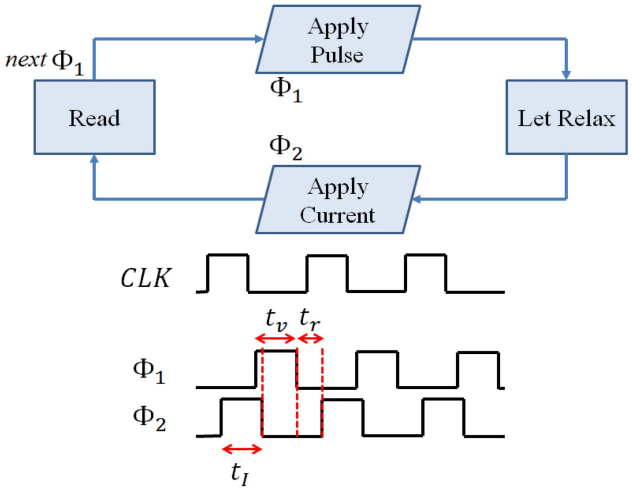

Fig. 4. Algorithm of the proposed TRNG with the control pulses.

create an energy barrier, which assumes its maximum along the minor axis ($\theta = \pi/2$) and its minimum along the major axis ($\theta = 0$ or $\theta = \pi$), as shown in Fig. 2(b). It should be noted that the second-order effects, such as exchange interactions, take negligible part in the total magnetic energy of the free layer compared with shape and uniaxial anisotropies [31]. For example, for our STR, in this paper, the exchange energy between the two magnetic layers contributes to less than 1% of the total magnetic energy of the device. Therefore, the energy level of parallel and antiparallel orientations can be assumed equal.

The resistance of an MTJ, R_{MTJ}, varies based on the relative magnetization orientation of the free and pinned layers. The conductance of the MTJ, $G_{\mathrm{MTJ}} = 1/R_{\mathrm{MTJ}}$, is given by

$$G_{\mathrm{MTJ}} = \frac{1}{2}(G_P + G_{\mathrm{AP}}) + \frac{1}{2}(G_P - G_{\mathrm{AP}})\cos\theta \qquad (1)$$

where G_P and G_{AP} are the conductance of the MTJ in the parallel and antiparallel orientations, respectively (associated with low and high resistance values of the MTJ, respectively). The PZT can be modeled as a parallel plate capacitance; therefore, the electrical model of the STR is a capacitance placed in series with a variable resistance, as shown in Fig. 2(c).

An applied voltage across the STR creates an electric field, which leads to a strain in the PZT due to piezoelectricity. The strain is transferred to the free layer as a physical stress. Depending on the polarity of the applied voltage, this external stress will act upon the intrinsic magnetic energy of the device and will reduce the energy barrier. If the applied voltage is higher than a critical value, known as the critical flipping voltage [26], V_C, the energy barrier will completely disappear; and the stress will force the magnetization vector to settle along the minor axis, as shown in Fig. 3(a). As long as the stress is acting on the magnet, the magnetization vector will stay along the minor axis, since this orientation minimizes the magnetic energy of the device. If the stress is removed abruptly, the device will suddenly enter a metastable state, since the minor axis is now the magnetic energy maximum. The thermal noise will now push the magnetization vector toward the parallel or antiparallel orientations. The dynamic waveforms of the above steps are shown in Fig. 3(b). The applied voltage will make the magnetization vector settle along the minor axis ($\theta = \pi/2$). Upon removal of the applied pulse, the magnetization will randomly settle into either a parallel state or an antiparallel state, leading to a low or high R_{MTJ}, respectively. This is the basis of our proposed TRNG based on the straintronics principle. MTJs can demonstrate endurances up to 10^{15} [32], and high endurance of the PZT can be achieved by applying unipolar pulses across the device [33]. Due to the capacitive nature of the PZT, the amount of leakage current flowing through the MTJ, while applying the voltage, is within a few nanoamperes; therefore, spin transfer torque (STT) effects are neglected.

Our proposed algorithm along with its timing information is shown in Fig. 4. Two pulses, Φ_1 and Φ_2, with the same frequencies and different phases are used throughout the process. The pulses are generated in a controller unit using a clock signal. There are four different phases for generating a random bit. In the first phase, the Φ_1 pulse is applied across the device until the magnetization vector of the STR settles along the minor axis. Then, the applied voltage is removed abruptly, allowing the magnetization vector to relax back along the major axis into either a parallel state or an antiparallel state. Depending on the parallel or antiparallel orientations, the MTJ will have a high or a low resistance value. Next, in order to read the final state of the STR, we apply a current through the MTJ and evaluate the voltage. A high or low voltage is associated with the logic bits 1 or 0, respectively. After reading the state, the same procedure for random bit generation continues to output the next bit.

III. Dynamic Modeling

In this section, we will first discuss the microspin modeling based on the Landau–Lifshitz–Gilbert (LLG) dynamics.

The effect of thermal noise will be discussed as it is the main contributor to the random final state of the STR. The effect of process variation on the energy barrier will be analyzed. Finally, we will study the speed of random number generation and the contributing factors into it. By investigating different material's flipping delays, we opt to find the proper candidate to develop a high-speed TRNG.

A. Dynamic Modeling of the Magnetization Vector's Behavior

The dynamic behavior of the magnetization vector, $\vec{M}$, is predicted using the LLG equation [34]

$$\frac{d\vec{M}}{dt} = -\gamma_0(\vec{M} \times \overrightarrow{H_{\text{eff}}}) - \frac{\alpha\gamma_0}{M_S}\vec{M} \times (\vec{M} \times \overrightarrow{H_{\text{eff}}}) \tag{2}$$

where γ_0 is the gyromagnetic ratio, α is the Gilbert damping factor, M_S is the saturation magnetization, and H_{eff} is the total magnetic field that is acting on the magnetization vector. The intrinsic magnetic anisotropies and the external forces, including the applied stress, contribute to H_{eff}.

The LLG equation can be simplified using the spherical coordinates with θ being the angle of the free layer's magnetization vector with the z-axis, and φ being the angle of the vector's x–y plane projection with the x-axis, as shown in Fig. 2(a). Since the magnetization vector, $\vec{M}$, is always pointing toward the $\hat{r}$ direction, there will be only two components of $\overrightarrow{H_{\text{eff}}}$ that act on the magnet: 1) $H_{\text{eff},\varphi}$ and 2) $H_{\text{eff},\theta}$. We have

$$\frac{d\theta}{dt} = \frac{\gamma_0}{1+\alpha^2}(H_{\text{eff},\varphi} + \alpha H_{\text{eff},\theta}) \tag{3a}$$

$$\frac{d\varphi}{dt} = \frac{\gamma_0}{1+\alpha^2}\frac{1}{\sin\theta}(\alpha H_{\text{eff},\varphi} - H_{\text{eff},\theta}) \tag{3b}$$

where the two factors, $H_{\text{eff},\varphi}$ and $H_{\text{eff},\theta}$, will be expressed as

$$H_\varphi = -\frac{1}{\mu_0 \text{VM}_S}\frac{1}{\sin\theta}\frac{\partial E}{\partial \varphi} \tag{4a}$$

$$H_\theta = -\frac{1}{\mu_0 \text{VM}_S}\frac{\partial E}{\partial \theta} \tag{4b}$$

in which, E is the total energy due to intrinsic magnetic anisotropies and the applied stress and is given by

$$E = \frac{\mu_0}{2}M_S^2 N_{\text{sh}} V + K_u V \sin^2\theta + \frac{3}{2}\lambda_S \sigma V \sin^2\theta_\sigma. \tag{5}$$

The first two terms relate to the shape and uniaxial anisotropies, respectively, and the third term is due to the applied stress. Here, μ_0 is the magnetic permeability of vacuum, N_{sh} is the demagnetization factor, V is the volume of the free layer, K_u is the uniaxial anisotropy coefficient, λ_S is the magnetostriction expansion at saturation, σ is the applied stress, and θ_σ is the angle between the magnetization vector and the minor axis.

Equation (3) is used to predict the magnetization vector's behavior under the applied stress at any time and provides the basis of our STR modeling. The parameters α and M_S in the LLG equation are material dependent and their values vary based on the magnetostrictive material used for the free layer of the MTJ.

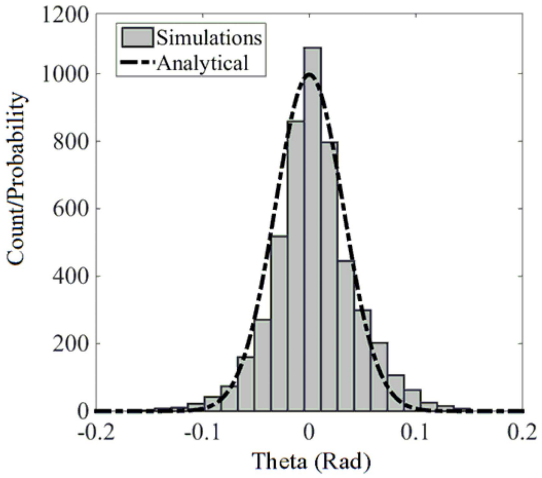

Fig. 5. Analytical and simulated initial angle due to the Langevin thermal noise.

B. Effect of Thermal Noise

Once the applied stress is removed abruptly, thermal noise will force the magnetization vector to rotate toward the parallel or antiparallel orientations. Therefore, an accurate model that closely mimics the effect of thermal noise should be incorporated into the LLG dynamics. This is done by incorporating the Langevin thermal noise field [35], [36], H_N, into (3). The incorporated field, which closely predicts the thermal noise behavior, is expressed as [35]

$$H_{N,i} = \sqrt{\frac{2\alpha kT}{\mu_0\gamma_0 M_s V}}X_i(t) \quad i = (x, y, z) \tag{6}$$

where k is the Boltzmann constant, T is the operating temperature, and $X_i(t)$ values are uncorrelated Gaussian distributions with zero mean and unit variance in three Cartesian directions.

The random noise field leads to fluctuations of the magnetization vector around the major axis in the absence of stress. It is demonstrated that these fluctuations have a Gaussian distribution with standard deviations of $\theta_{\text{rms}} = (kT/\mu_0 \text{VM}_s H_{\text{eff}})^{1/2}$ [37]. Our simulation data after the incorporation of thermal noise into the model along with the expected analytical data are shown in Fig. 5. The accuracy of the model is confirmed by comparing the two graphs.

C. Effect of Process Variation

Process variation can have a variety of impacts on the STR. While most of these effects might manipulate the TMR ratio or the maximum and minimum resistance values of the MTJ, the major effect that can lead to TRGN failure is the loss of energy barrier between the parallel and the antiparallel states, as shown in Fig. 6(a). If the dimensions of the free layer are chosen closely, such that the energy barrier is small, then process variation can swap the major and minor axes of the device, as shown in the figure, making $\theta = \pi/2$ the preferred orientation of the magnetization vector in the absence of stress. In this case, applying stress across the STR will not lead to switching as the PZT will further force the magnetization vector to stay along the y-axis. In order to prevent this, the major axis and minor axis dimensions (a and b,

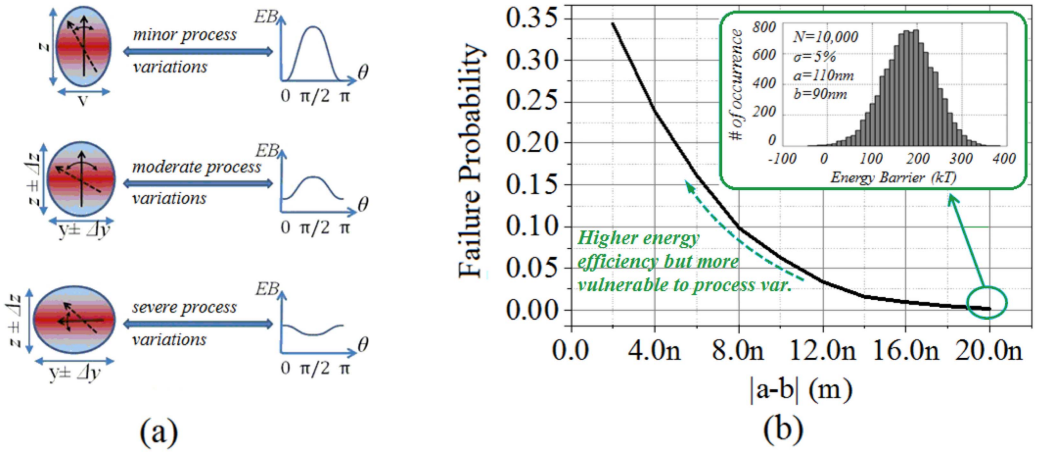

Fig. 6. (a) Effect of process variation: a severe process variation can swap the axis and remove the energy barrier. (b) Failure due to process variation as a function of axis dimensions. As the device's dimensions become more circular, the failure rate raises while the energy efficiency increases.

respectively, where: $a > b$) should be selected to provide a high-energy barrier. The dimensions are selected based on the available process variation, which is technology dependent. The selection of dimensions, however, can affect the energy barrier of the device. Therefore, an energy-reliability tradeoff exists when it comes to the device geometry. If $a \gg b$, a higher energy is required for the STR switching, translating to a higher immunity against process variation failures. The values of a close to b reduce the energy barrier in expense of a higher vulnerability to process variations. In Fig. 6(b), failure is defined as the probability of $a < b$ under a process variation with a Gaussian distribution, where stdv $= 5\%$, which is a conservative assumption in a 65 nm process technology [38]. As demonstrated in the figure, the selected dimensions, $a = 110$ nm and $b = 90$ nm, provide enough immunity against process variation, leading to less than 2×10^{-4} failure probability.

D. TRNG Performance and the Choice of Magnetostrictive Material

Three different delays contribute to the timing diagram in Fig. 4 and dominate the speed of the TRNG.

1) t_v: The time required for the magnetization vector to rotate and settle along the minor axis. This delay is material and voltage dependent, as shown in Fig. 7, where we simulated the flipping delay of five different materials as a function of the applied voltage. Due to the parameters in (2), various materials demonstrate different delays. Metglas and Cobalt show slower responses, while Galfenol and Terfenol-D are the faster candidates, mainly due to their higher magnetostriction coefficient. However, it should be noted that a higher applied voltage can contribute to more oscillations of the magnetization vector while settling along the minor axis [26]; therefore, it is not always helpful to increase the voltage level to get a faster response.
2) t_r: The time required for the magnetization vector to relax along the major axis after the pulse is removed. There is no voltage dependence here, and t_r is solely material dependent. The values of t_r for different materials are enumerated in Table I, where Galfenol is observed to relax back toward the major axis much faster than the other materials owing to its higher shape anisotropy energy.
3) t_I: The time required to reach a steady voltage on the top of the MTJ when the current is flown through the device. This is a function of the resistance of the MTJ and the capacitance of the readline, which mainly consists of the PZT capacitance. Therefore, t_I does not mainly depend on the magnetostrictive material.

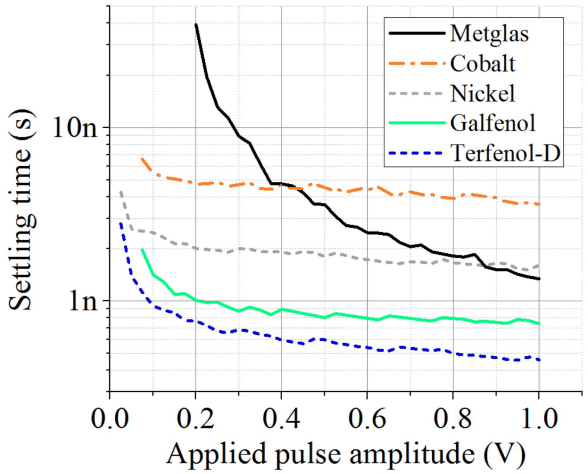

Fig. 7. Settling time as a function of the applied voltage amplitude for different materials.

As a result of the above discussions, Galfenol is chosen as the primary choice of the magnetostrictive material due to its fast response to the applied voltage and its quick relaxation time. This assures a fast pace for the random bit generation in our proposed TRNG.

IV. TRNG Cell Design

CMOS circuitry can be used in order to generate the required control signals in Fig. 4 and to assist with reading

TABLE I
SETTLING AND RELAXATION TIME FOR DIFFERENT MATERIALS

	Terfenol-D	Nickel	Cobalt	Galfenol	Metglas
$t_r(ns)^*$	2.62	2.76	2.06	1.16	4.66
$t_v(ns)^*$	0.60	1.90	4.55	0.80	3.60

* The settling criteria is set to $\pi/10$ of the final state

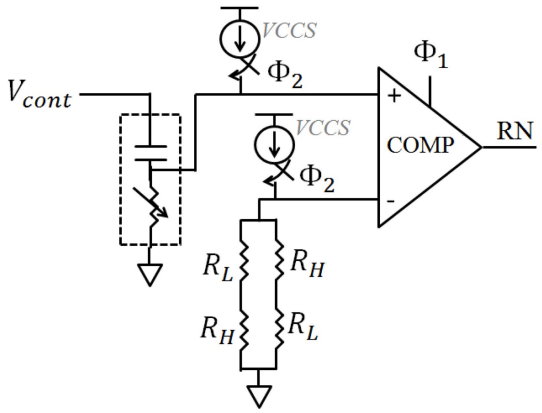

Fig. 8. Proposed schematic of the TRNG bitcell. R_H and R_L are the high- and low-resistance states in the antiparallel and parallel orientations, respectively ($R_H = 1/G_{\text{AP}}$ and $R_L = 1/G_P$).

the state of the MTJ. The proposed cell design that generates one random bit per clock cycle is shown in Fig. 8. The signals V_{cont}, Φ_1, and Φ_2 are generated from a clock using a delay block. The STR is a three-port device [27], as shown in the figure, where the top plate voltage, V_{cont}, is used to apply a high voltage across the device and push the STR into the metastable state. The side port is solely used for reading the MTJ resistance and is inactive when V_{cont} is pushing the cell into metastability. Upon removal of V_{cont}, the device will settle randomly either into a parallel state or into an antiparallel state. Then, the current that is generated in voltage-controlled current sources (VCCSs) will flowthrough the MTJ in the Φ_2 phase. Then, the comparator will determine the state of the STR by comparing it to the reference cell. The comparator uses a digital latched topology [39], and the differential pair is oversized to alleviate the offset due to mismatch [40]. Our analysis based on the Pelgrom law [40] predicts more than 95% success when the comparator is subject to mismatch due to process variations. Here, success is associated with the cases where the comparator's offset due to mismatch is below the voltage difference between the STR and the reference cell in Fig. 8, leading to comparator's successful comparison.

The VCCS current level is maintained within a few microamperes for two purposes: 1) to keep the read energy low by restricting the total current driven from the VCCS over the entire read operation and 2) to assure that no STT effect will happen [41]. The STT effect can cause an unwanted change in the state of the MTJ (read disturb). The reference cell is made with the MTJs that are pinned into the parallel and antiparallel states; therefore, the equivalent reference resistance will be $[(R_H + R_L)/2]$.

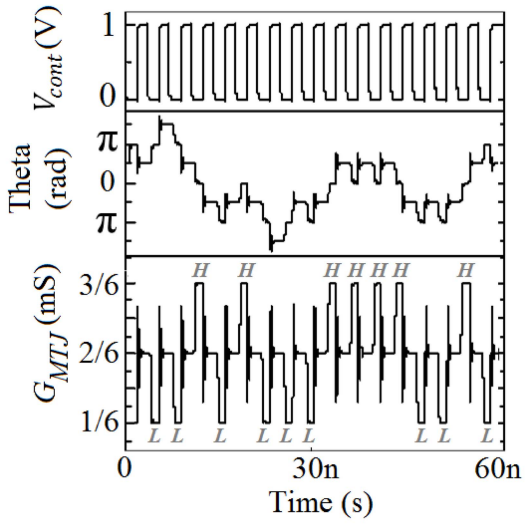

Fig. 9. Demonstration of the random final conductance state of the MTJ when a rail of pulses is applied across the device.

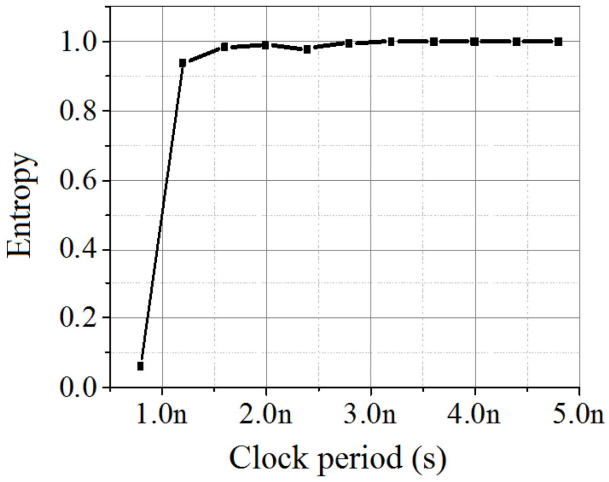

Fig. 10. Entropy of the TRNG bitcell as a function of the clock period.

Fig. 9 shows the random conductance generation (high or low) using the proposed bitcell. When the voltage V_{cont} goes high, the magnetization vector rests on the minor axis, where $\theta = (2i+1)\pi/2$. This means the MTJ conductance will settle to its middle value. Upon resetting V_{cont}, θ will settle along $2i\pi$ or $(2i+1)\pi$, leading to a low or high conductance value. For clarity, the final conductance level is also shown in the figure.

The highest rate at which the bitcell can generate random numbers is dictated by t_v, t_r, and t_I. This sets a minimum value on the clock period. If the period is shortened further, the magnetization vector of the free layer under stress will not have enough time to settle along the minor axis (shortage of t_v). Therefore, random number generation will not be guaranteed at very small clock period values, since the system will not settle into the metastable state. This dependence of the randomness on the clock period is shown in Fig. 10, where the entropy, H, of the random number generation is

TABLE II
COMPARISON OF THE PROPOSED TRNG WITH THE WORKS IN THE LITERATURE

	[6]	[8]	[9]	[10]	[12]	This work	
Method	Back-to-back inverter loop	Fast clock and slow jittery clock	Fast and slow jittery clock with discrete-time chaos	Metastable dynamic latch	Synthesized 3-satge ring oscillator	Straintronics metastability	
CMOS process	45nm	180nm	2um	0.35um	28nm	65nm	
VDD (V)	1.1	1.8	3	5	0.9	1	0.5
Energy/bit (J)	2.9p	230p	3.9n	1.88n	23p	0.125p	0.019p
Maximum frequency (Hz)	2.4G	10M	1.4M	5K	23M	510MHz	110MHz
Area(mm^2)	0.004	0.0016	1.5	0.031	0.000375	0.001*	

*Estimated area of the design by calculating the total area of the CMOS peripheral controller and sensing circuitries and switches. The straintronics devices can lie on top of CMOS circuitry to help maximize area efficiency

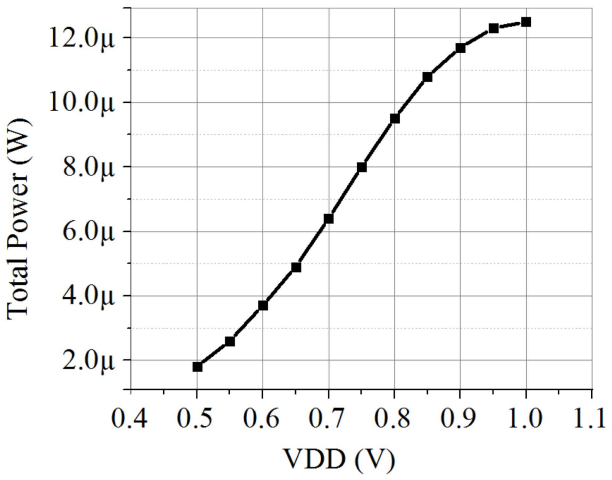

Fig. 11. Total power of the TRNG as a function of V_{DD}; the power includes the CMOS peripherals.

TABLE III
NIST RANDOMNESS TEST ON 100 kb OF THE PROPOSED STR TRNG

Test	Proportion*	Result?
Frequency	10/10	PASS
Block Frequency	10/10	PASS
Cumulative sums (forward)	10/10	PASS
Cumulative sums (reverse)	10/10	PASS
Runs	10/10	PASS
Longest run of ones	10/10	PASS
Rank	10/10	PASS
FFT	9/10	PASS
Non-overlapping templates	All sub-tests PASS	
Overlapping template	10/10	PASS
Approximate entropy	9/10	PASS
Serial	10/10	PASS
Linear Complexity	10/10	PASS

* Minimum passing rate of 8 for a sample size of 10 binary sequences, according to NIST test suit.

defined as

$$H = -p(1) \times \log_2 p(1) - p(0) \times \log_2 p(0) \tag{7}$$

where $p(0)$ and $p(1)$ are the probabilities of observing logic 0 and 1. As a result, the clock periods below 2 ns can cause low entropy values and are avoided.

V. SIMULATION RESULTS

The RNG cell, introduced in Section IV, demonstrates high performance while retaining low values of energy and power dissipation. It is necessary to mention that the leakage power through the STR will be low as well due to the capacitive nature of the PZT. Therefore, the main source of leakage will be the CMOS control circuitry. At 1 V supply level, the circuit can generate random bits at speeds up to 510 MHz. The entire circuit, including the CMOS peripherals, dissipates 12.5 uW total power at 100 MHz throughput rate. At this rate, the system consumes 125 fJ/bit for random bit generation which is approximately 23× lower than the state-of-the-art CMOS RNG [6].

The total power of the system as a function of V_{DD} is shown in Fig. 11. By reducing the power supply to 0.5 V (near-threshold operation for the CMOS), the total power reduces to merely 1.9 uW, corresponding to 19 fJ/bit. Significant power savings are achieved by reducing the supply voltage since that would push the VCCSs into the subthreshold operation regime. The latter can make the system the optimum candidate for energy-limited low-voltage applications. A comparison between the straintronics TRNG and the state-of-the-art TRNG hardware in terms of speed, energy efficiency, and area is provided in Table II. Major energy savings are accomplished due to the inherent energy efficiency of the STR devices.

In order to test the reliability of the generated random numbers, the straintronics TRNG was tested using the National Institute of Standards and Technology (NIST)standard platform, and the results are reported in Table III. The proposed TRNG passes the performed NIST tests (meant for high security cryptographic systems), indicating the true randomness of the generated data.

VI. CONCLUSION

We exploited the metastability feature of the straintronics device in order to design an energy-efficient TRNG that merely dissipated 125 fJ per bit at the 1 V supply level. The system can generate random numbers as fast as 510 MHz. The TRNG

can operate at the near-threshold regime while dissipating 19 fJ per bit at the 0.5 V supply level. Due to the high energy efficiency and high performance, the straintronics-based TRNG can be the optimal candidate for both the high-speed and energy-limited applications.

ACKNOWLEDGMENT

This work was supported in part by the Air Force Office of Scientific Research under Grant FA9550-12-1-0402 and in part by the Nanoelectronics for 2020 and Beyond Program through the National Science Foundation under Grant ECCS-1124714 (PT106594-SC103006).

REFERENCES

[1] Z. Gutterman, B. Pinkas, and T. Reinman, "Analysis of the Linux random number generator," in *Proc. IEEE Symp. Secur. Privacy*, May 2006, pp. 371–385.

[2] M. Lüscher, "A portable high-quality random number generator for lattice field theory simulations," *Comput. Phys. Commun.*, vol. 79, no. 1, pp. 100–110, 1994.

[3] S. K. Park and K. W. Miller, "Random number generators: Good ones are hard to find," *Commun. ACM*, vol. 31, pp. 1192–1201, Oct. 1988.

[4] M. Matsumoto and T. Nishimura, "Mersenne twister: A 623-dimensionally equidistributed uniform pseudo-random number generator," *ACM Trans. Model. Comput. Simul.*, vol. 8, pp. 3–30, Jan. 1998.

[5] G. A. Lopez, M. Taufer, and P. J. Teller, "Evaluation of IEEE 754 floating-point arithmetic compliance across a wide range of heterogeneous computers," in *Proc. Conf. Diversity Comput. (TAPIA)*, 2007, pp. 1–4.

[6] S. K. Mathew *et al.*, "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.

[7] C. Tokunaga, D. Blaauw, and T. Mudge, "True random number generator with a metastability-based quality control," *IEEE J. Solid-State Circuits*, vol. 43, no. 1, pp. 78–85, Jan. 2008.

[8] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, "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.

[9] 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.

[10] J. Holleman, S. Bridges, B. P. Otis, and C. Diorio, "A 3 μW CMOS true random number generator with adaptive floating-gate offset cancellation," *IEEE J. Solid-State Circuits*, vol. 43, no. 5, pp. 1324–1336, May 2008.

[11] C. De Roover and M. Steyaert, "A 500 mV 650 pW random number generator in 130 nm CMOS for a UWB localization system," in *Proc. ESSCIRC*, Sep. 2010, pp. 278–281.

[12] 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. Dig. Tech. Papers (ISSCC)*, Feb. 2014, pp. 280–281.

[13] F. Pareschi, G. Setti, and R. Rovatti, "Implementation and testing of high-speed CMOS true random number generators based on chaotic systems," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 57, no. 12, pp. 3124–3137, Dec. 2010.

[14] R. Yeniçeri and M. E. Yalçin, "True random bit generation with time-delay sampled-data feedback system," *Electron. Lett.*, vol. 49, no. 8, pp. 543–545, Apr. 2013.

[15] P. Z. Wieczorek and K. Golofit, "Dual-metastability time-competitive true random number generator," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, no. 1, pp. 134–145, Jan. 2014.

[16] P. Z. Wieczorek, "An FPGA implementation of the resolve time-based true random number generator with quality control," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, no. 12, pp. 3450–3459, Dec. 2014.

[17] H.-T. Yang, J.-R. Huang, and T.-Y. Chang, "A chaos-based fully digital 120 MHz pseudo random number generator," in *Proc. IEEE Asia-Pacific Conf. Circuits Syst.*, vol. 1. Dec. 2004, pp. 357–360.

[18] F. Weiss, H.-D. Wohlmuth, D. Kehrer, and A. L. Scholtz, "A 24-Gb/s 2^7–1 pseudo random bit sequence generator IC in 0.13 μm bulk CMOS," in *Proc. 32nd Eur. Solid-State Circuits Conf. (ESSCIRC)*, Sep. 2006, pp. 468–471.

[19] W. Zhao, E. Belhaire, and C. Chappert, "Spin-MTJ based non-volatile flip-flop," in *Proc. 7th IEEE Conf. Nanotechnol. (IEEE-NANO)*, Aug. 2007, pp. 399–402.

[20] S. Matsunaga *et al.*, "Fabrication of a nonvolatile full adder based on logic-in-memory architecture using magnetic tunnel junctions," *Appl. Phys. Exp.*, vol. 1, no. 9, p. 091301, Aug. 2008.

[21] M. Kamiyanagi *et al.*, "Transient characteristic of fabricated magnetic tunnel junction (MTJ) programmed with CMOS circuit," *IEICE Trans. Electron.*, vol. E93-C, no. 5, pp. 602–607, 2010.

[22] R. Nebashi *et al.*, "A 90 nm 12 ns 32 Mb 2T1MTJ MRAM," in *IEEE Int. Solid-State Circuits Conf.-Dig. Tech. Papers (ISSCC)*, Feb. 2009, pp. 462–463 and 463a.

[23] K. Roy, S. Bandyopadhyay, and J. Atulasimha, "Hybrid spintronics and straintronics: A magnetic technology for ultra low energy computing and signal processing," *Appl. Phys. Lett.*, vol. 99, no. 6, p. 063108, 2011.

[24] A. Khan, D. E. Nikonov, S. Manipatruni, T. Ghani, and I. A. Young, "Voltage induced magnetostrictive switching of nanomagnets: Strain assisted strain transfer torque random access memory," *Appl. Phys. Lett.*, vol. 104, no. 26, pp. 262407-1–262407-5, Jun. 2014.

[25] M. Barangi and P. Mazumder, "Straintronics-based random access memory as universal data storage devices," *IEEE Trans. Magn.*, vol. 51, no. 5, May 2015, Art. ID 3400408.

[26] M. Barangi and P. Mazumder, "Straintronics-based magnetic tunneling junction: Dynamic and static behavior analysis and material investigation," *Appl. Phys. Lett.*, vol. 104, no. 16, pp. 162403-1–162403-5, Apr. 2014.

[27] M. Barangi and P. Mazumder, "Straintronics: A leap toward ultimate energy efficiency of magnetic random access memories," *IEEE Nanotechnol. Mag.*, vol. 9, no. 3, pp. 15–24, Sep. 2015.

[28] S.-K. Kim, S.-C. Shin, and K. No, "Voltage control of magnetization easy-axes: A potential candidate for spin switching in future ultrahigh-density nonvolatile magnetic random access memory," *IEEE Trans. Magn.*, vol. 40, no. 4, pp. 2637–2639, Jul. 2004.

[29] N. Lei *et al.*, "Strain-controlled magnetic domain wall propagation in hybrid piezoelectric/ferromagnetic structures," *Nature Commun.*, vol. 4, Jan. 2013, Art. ID 1378.

[30] N. D'Souza, M. S. Fashami, S. Bandyopadhyay, and J. Atulasimha. (Apr. 2014). "Experimental clocking of nanomagnets with strain for ultra low power Boolean logic." [Online]. Available: http://arxiv.org/abs/1404.2980

[31] L. Engelbrecht, "Modeling spintronics devices in Verilog-A for use with industry standard simulation tools," Ph.D. dissertation, School Elect. Eng. Comput. Sci., Oregon State Univ., Corvillis, OR, USA, Mar. 2011.

[32] S. Tehrani *et al.*, "Magnetoresistive random access memory using magnetic tunnel junctions," *Proc. IEEE*, vol. 91, no. 5, pp. 703–714, May 2003.

[33] A. L. Kholkin, E. L. Colla, A. K. Tagantsev, D. V. Taylor, and N. Setter, "Fatigue of piezoelectric properties in $Pb(Zr, Ti)O_3$ films," *Appl. Phys. Lett.*, vol. 68, no. 18, pp. 2577–2579, Apr. 1996.

[34] S. Chikazumi, *Physics of Ferromagnetism*. London, U.K.: Oxford Univ. Press, Feb. 1997.

[35] W. F. Brown, Jr., "Thermal fluctuations of a single-domain particle," *J. Appl. Phys.*, vol. 34, no. 4, pp. 1319–1320, Apr. 1963.

[36] G. Grinstein and R. H. Koch, "Coarse graining in micromagnetics," *Phys. Rev. Lett.*, vol. 90, no. 20, p. 207201, May 2003.

[37] S. Manipatruni, D. E. Nikonov, and I. A. Young, "Modeling and design of spintronic integrated circuits," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 59, no. 12, pp. 2801–2814, Dec. 2012.

[38] S. Shedabale, H. Ramakrishnan, G. Russell, A. Yakovlev, and S. Chattopadhyay, "Statistical modelling of the variation in advanced process technologies using a multi-level partitioned response," *IET Circuits, Devices, Syst.*, vol. 2, no. 5, pp. 451–464, Oct. 2008.

[39] T. Kobayashi, K. Nogami, T. Shirotori, and Y. Fujimoto, "A current-controlled latch sense amplifier and a static power-saving input buffer for low-power architecture," *IEEE J. Solid-State Circuits*, vol. 28, no. 4, pp. 523–527, Apr. 1993.

[40] M. J. M. Pelgrom, A. C. J. Duinmaijer, and A. P. G. Welbers, "Matching properties of MOS transistors," *IEEE J. Solid-State Circuits*, vol. 24, no. 5, pp. 1433–1439, Oct. 1989.

[41] D. C. Ralph and M. D. Stiles, "Spin transfer torques," *J. Magn. Magn. Mater.*, vol. 320, no. 7, pp. 1190–1216, 2008.

Mahmood Barangi received the B.S. degree in electrical engineering from the Sharif University of Technology, Tehran, Iran, in 2009, and the M.S. degree in electrical engineering from the University of Michigan, Ann Arbor, MI, USA, in 2011, where he is currently pursuing the Ph.D. degree.

He is a Graduate Student Research Assistant with the Electrical Engineering and Computer Science Department, University of Michigan. His current research interests include low power digital and mixed signal circuit design, SRAM memory design, and spin transfer torque-based logic and memory design.

Joseph S. Chang (M'04) received the B.Eng. degree in electrical and computer engineering from Monash University, Melbourne, VIC, Australia, and the Ph.D. degree from the Department of Otolaryngology, University of Melbourne, Melbourne.

He is currently with Nanyang Technological University, Singapore, where he was the Associate Dean of Research and Graduate Studies with the College of Engineering. He is also an Adjunct Professor with Texas A&M University, College Station, TX, USA. He is a Multidisciplinary Engineer. He has founded two startups in the field of electroacoustics, and has designed numerous related products, adopted for the industry and commercial products. He publishes prolifically and holds ten patents with several pending. His current research interests include emerging technologies and traditional circuits and system-related fields, including printed electronics, microfluidics, life sciences, audiology, psychophysics, acoustics, and biomedical and electronic devices.

Dr. Chang serves as an Editor of the *IEEE Circuits and Systems Magazine* (Open Column), and is an Associate Editor of the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS I. He was a Guest Editor of the PROCEEDINGS OF THE IEEE. He is the Chair of the Life Sciences Systems and Applications Technical Committee of the IEEE Circuits and Systems (CAS) Society, and was an Associate Editor of the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS II. He has chaired several international conferences, including the IEEE National Institutes of Health (NIH) Life Sciences Systems and Applications Workshop, the IEEE NIH CAS Medical and Environmental Workshop, and the International Symposium on Integrated Circuits and Systems. He has received numerous academic, defense, and industrial grants, exceeding U.S. $11 million, including from the Defense Advanced Research Projects Agency, Arlington, VA, USA, E.U. grants, and multinational corporations.

Pinaki Mazumder (S'84–M'87–SM'95–F'99) received the Ph.D. degree from the University of Illinois at Urbana–Champaign, Champaign, IL, USA, in 1988.

He was with industrial research and development centers for six years that included AT&T Bell Laboratories, Murray Hill, NJ, USA, where he started the CONES Project—the first C modeling-based very large scale integration (VLSI) synthesis tool with India's premier electronics company, Bharat Electronics, Ltd., Chennai, India, in 1985, where he had developed several high-speed and high-voltage analog integrated circuits intended for consumer electronics products. He is currently a Professor with the Department of Electrical Engineering and Computer Science, University of Michigan (UM), Ann Arbor, MI, USA. He is on leave for one year from UM to serve as the Lead Program Director of the Emerging Models and Technologies Program with the U.S. National Science Foundation, Arlington, VA, USA. He has authored or co-authored over 200 technical papers and four books in various aspects of VLSI research studies. His current research interests include current problems in nanoscale CMOS VLSI design, computer-aided design tools, and circuit designs for emerging technologies, including quantum MOS and resonant tunneling devices, semiconductor memory systems, and physical synthesis of VLSI chips.

Dr. Mazumder was a fellow of the American Association for the Advancement of Science in 2008. He was a recipient of the Digital's Incentives for Excellence Award, the BF Goodrich National Collegiate Invention Award, and the Defense Advanced Research Projects Agency Research Excellence Award.