Superparamagnetic perpendicular magnetic tunnel junctions for true random number generators

Cite as: AIP Advances **8**, 055903 (2018); https://doi.org/10.1063/1.5006422
Submitted: 25 September 2017 • Accepted: 16 October 2017 • Published Online: 07 December 2017

Bradley Parks, Mukund Bapna, Julianne Igbokwe, et al.

Superparamagnetic perpendicular magnetic tunnel junctions for true random number generators

Bradley Parks,[1] Mukund Bapna,[1] Julianne Igbokwe,[1] Hamid Almasi,[2] Weigang Wang,[2] and Sara A. Majetich[1,a]
[1]*Department of Physics, Carnegie Mellon University, Pittsburgh, PA 15235, USA*
[2]*Department of Physics and Astronomy, University of Arizona, Tucson, AZ 85721, USA*

(Presented 9 November 2017; received 25 September 2017; accepted 16 October 2017; published online 7 December 2017)

Superparamagnetic perpendicular magnetic tunnel junctions are fabricated and analyzed for use in random number generators. Time-resolved resistance measurements are used as streams of bits in statistical tests for randomness. Voltage control of the thermal stability enables tuning the average speed of random bit generation up to 70 kHz in a 60 nm diameter device. In its most efficient operating mode, the device generates random bits at an energy cost of 600 fJ/bit. A narrow range of magnetic field tunes the probability of a given state from 0 to 1, offering a means of probabilistic computing. https://doi.org/10.1063/1.5006422

I. INTRODUCTION

Encryption is vital to protecting everything from personal data to financial transactions to national security information., and recent high profile compromises of data security highlight the need for better encryption. Due to their limited speed, large area, and high power consumption, it is not feasible to generate *true* random numbers fast enough for real-time encryption, hence hardware random number generators (RNGs) are used to seed *pseudo*-random number generating algorithms. The steady growth of processing power necessitates ever-larger encryption keys. Superparamagnetic perpendicular magnetic tunnel junctions (SP-pMTJs) offer a low power, dense alternative to current hardware RNG technology. Here we fabricate RNGs and test the randomness of their output.

The current technology for hardware RNGs is the free running oscillator ring. These RNGs use phase jitter arising from the changing temperature of the silicon in a series of NOT gates as a source of electronic noise that is thereby used to generate random bits.[1] The frequency of the ring oscillator is set by the capacitive lag as the gates of the MOSFETs charge in series. The output is read at a rate set by an external clock, which has its own inherent uncertainty. The variability of the frequencies in the ring oscillator and clock give rise to a random walk in their relative phase, with the frequency of each component being dependent on the temperature. These circuits are typically hundreds of square microns, consume milliwatts of power, and generate tens to hundreds of megabits per second.[2] Recent experiments in CMOS based RNGs have increased the speed to a few gigabits per second and reduced area by a factor of ten, but without significant reduction in power consumption.[3]

Previous work on superparamagnetism has mainly focused on nanoparticles.[4] Recently, superparamagnetic magnetic tunnel junctions (SP-MTJs) have been proposed for use in RNGs. Experimental work has been done using in-plane SP-MTJs in which random bits were produced by 50 x150 nm^2 devices at a rate of 1.66 kHz and an energy cost of about 2.5 fJ/bit.[5] However, dense arrays of in-plane devices would have significant magnetostatic interactions that could compromise the randomness of their outputs. There has been some simulation work done to suggest that low

[a]Corresponding author: sara@cmu.edu

thermal stability perpendicular MTJs (pMTJs) can be used to create highly parallel random number generators with small process size, high density, low power, and high throughput.[6] Perpendicular MTJs can be scaled down to 20nm or smaller[7] and can be patterned with smaller pitch/higher density.[8] Here we present experimental results from a 60nm hardwired SP-pMTJ used as a true random number generator with voltage tunable frequency.

II. EXPERIMENTAL METHODS

Perpendicular MTJs were used to capitalize on voltage controlled magnetic anisotropy (VCMA). A film stack of Si/Ta(5)/Ru(10)/Ta(5)/$Co_{20}Fe_{60}B_{20}$(0.85)/MgO(~1.5)/$Co_{40}Fe_{40}B_{20}$(1.5)/Ta(5)/Ru(8) was deposited by magnetron sputtering. Here the numbers in parentheses are the film thicknesses in nanometers. The film was annealed at 300°C for 10 minutes. 60 nm diameter MTJ pillars were defined by electron beam lithography and Ar ion milling, and leads and bond pads were defined by photolithography.

The sample was then placed in a chip carrier and wire bonded, in order to connect individual devices to a voltage source and ammeter. Bias was applied through the bottom lead while the top was grounded. Thus, for negative bias, electrons flow upward from the fixed reference layer toward the low thermal stability reference layer.

A MTJ-based RNG should spend equal amounts of time in the parallel (P) and antiparallel (AP) states, and therefore the stray field due to the fixed layer should be offset. In small diameter MTJs this field can be hundreds of Oe. The minor loop tunnel magnetoresistance as a function of magnetic field was measured to determine the magnitude of this stray field for a given device, and an external field in the opposite direction was then applied to cancel it. The data was acquired at an acquisition frequency of 100 MHz for 500 ms to get statistically significant number of switches.

III. RESULTS AND DISCUSSION

Figure 1 shows some sample time traces collected at different bias values. The tunnel magnetoresistance (TMR) ranged from 10% at -1.3 V to 35% at -0.4 V. For a given voltage, the separation between the states was used to threshold and digitize the signal as ones (high resistance) or zeros (low resistance).

Thermally driven magnetization reversal of a superparamagnet is described by a Néel relaxation model, with a relaxation time given by $\tau = \tau_0 \exp[K_{eff}\ V/k_B T]$, where τ is the average time spent in the state, τ_0 is the inverse of the Larmor precession frequency, K_{eff} is the effective anisotropy, V is the volume, k_B is the Boltzmann constant, and T is the temperature. For the SP-MTJ, the hopping process between P and AP state follows Poisson statistics and hence the distribution of time duration between switching events is exponential. From the fit of the exponential distribution, the lifetimes τ_P and τ_{AP}, corresponding to average times in the P and AP states, were obtained.

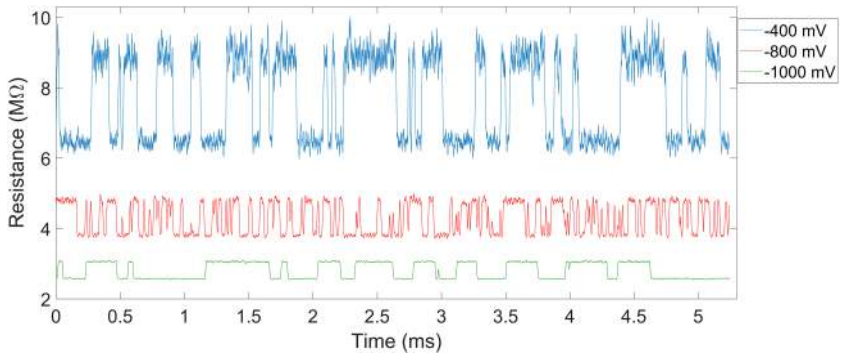

FIG. 1. The time varying resistance of the MTJ changes amplitude and frequency as a function of bias. Here an external field of 15.6 Oe was applied to cancel the stray field.

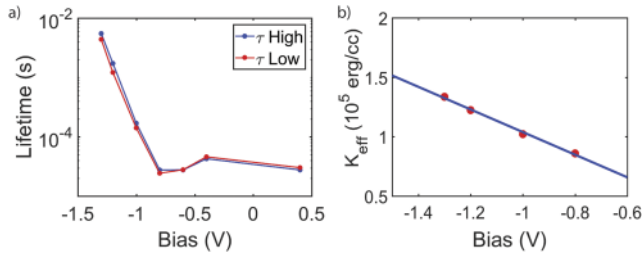

FIG. 2. a) The lifetime of the high and low current states vary nonlinearly with bias. b) In the linear regime, the effective anisotropy changes with a VCMA coefficient of 21 fJ/Vm.

Figure 2a shows the lifetime of the high and low current states as a function of bias. The time the device spends in each state is a nonlinear function of bias. The trend is linear and steep for large negative bias, but relatively unchanging for bias values more positive than about -800 mV. Using the Néel relaxation model, we can calculate how the bias affects the thermal stability factor, Δ. Figure 2b shows that the thermal stability is tunable with bias from 14.7 at -1.3 V to 9.5 at -0.8 V. The voltage controlled magnetic anisotropy (VCMA) coefficient is 21 fJ/Vm. In the maximum efficiency case of -0.4 V, the device operates at a power of 27 nW and an average speed of 45 kHz, thus the device produces random bits at an energy cost of 600 fJ per bit. The -0.4V case also offers the highest signal with a TMR ratio of about 35%.

The data stream was then analyzed for randomness by a number of methods from the NIST Statistical Test Suite.[9] For the analysis of randomness, the data were sampled at intervals of $\tau = (\tau_P^{-1} + \tau_{AP}^{-1})^{-1}$. The left column of Table 1 lists the different tests. If a p-value >0.01 (significance level) is found for a particular test then the input bit stream is characterized as random as far as that test is concerned. For a RNG under test to qualify as a true RNG, a bit stream produced by it should pass through all the NIST STS tests.

An XOR whitening process was then applied to get rid of any bias for the device being in state 0 or 1. This bias in probability of the device being in P or AP state originate from the fact that the stray field from the bottom layer can favors P state over AP state. This bias can be large if the bottom layer is patterned,[10] however, here the effect is small since the reference layer was not patterned through. In an actual device, this effect can be mitigated all together, for example, by having a synthetic antiferromagnet structure with the reference layer to cancel the stray field.

The effect of different XOR whitening process is shown in Table 1. The bit stream for each bias value was separated into equal pieces to be input into a logical exclusive or operation. For XOR2, the data is divided into two streams and fed into an XOR, and the output is then used for the statistical testing. XOR4 and XOR8 use four and eight inputs, respectively. In a real application, these inputs could come from different tunnel junctions in parallel. The p-value for each test is shown for the

TABLE I. The NIST STS tests for randomness were applied to the time-resolved resistance measurements with different degrees of whitening. Bold-faced p-values indicate a passed test.

		-800 mV		-400 mV		
Test	Failure Criteria[11]	XOR2	XOR4	XOR2	XOR4	XOR8
Frequency	Total number of 0's and 1's mismatch	**0.597**	**0.984**	**0.656**	**0.242**	**0.649**
Block Frequency	Number of 0's and 1's mismatch within a subset	**0.030**	**0.328**	0	**0.861**	**0.344**
Cumulative Sums Forward	Running sum deviates too far from half the length	**0.877**	**0.950**	**0.705**	**0.379**	**0.798**
Cumulative Sums Reverse	Same as previous, but in reverse direction	**0.419**	**0.939**	**0.345**	**0.194**	**0.862**
Runs	Too many sequences of consecutive bits of one type.	0	**0.889**	0	0	**0.982**
Longest Run	Too many consecutive bits of one type	0	**0.846**	0	0.010	**0.773**
Approximate Entropy	Bit sequence too unlikely	0	**0.801**	0	0	**0.800**
Serial	Multiple low entropy sequences in a row	0	**0.573**	0	0	**0.653**
FFT	Periodicity in bit stream	**0.544**	**0.745**	0	**0.876**	**0.032**

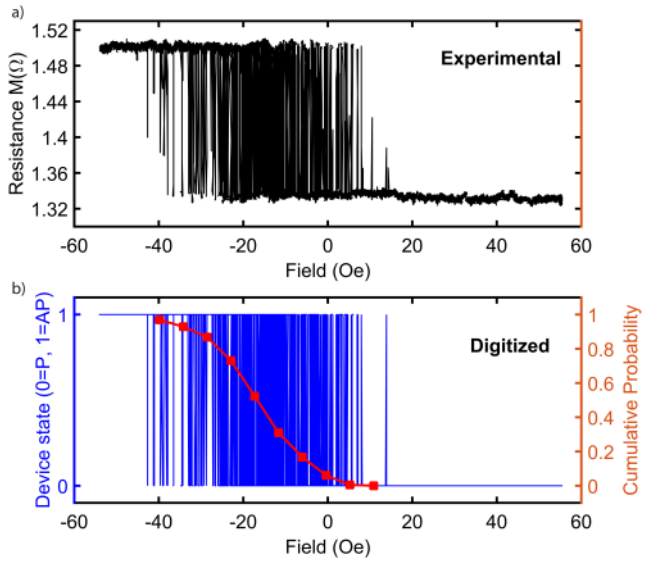

FIG. 3. a) A minor hysteresis loop acquired at -1.3 V showing the coercivity (half width of loop) and stray field (loop center) of the device. The free layer is telegraphing throughout the measurement. b) The digitized minor loop with a superimposed average magnetization (sigmoid) found from integration of the minor loop. Using the applied magnetic field, we can make the device favor one state rather than being approximately unbiased as in the time-resolved measurements.

highest speed case (-800 mV) and the most energy efficient case (-400 mV). Bold values indicate passing the test for randomness. For our data set, XOR2 whitening is effective only for large negative bias values, XOR4 is successful for biases from -1.3 V to -0.8 V, and XOR8 is sufficient to yield random bit streams in all cases.

Figure 3a shows a resistance versus applied magnetic field minor loop. An applied magnetic field initialized the free layer in one resistance state and was then swept at a rate of 60 Oe/s until the free layer was stable in the other state. In the middle region of the figure, the free layer switches thermally between the two resistance states with the highest frequency of switching where the applied field exactly cancels the stray field of the fixed layer. The average magnetization was controlled by the applied field, as shown in Figure 3b. Using an applied magnetic field range of just 60 Oe, we can tune the probability of reading the high resistance state from 0 to 1.

IV. CONCLUSION

We have shown SP-pMTJs can be used as true random number generators. These RNG devices operate at much lower power than current CMOS oscillator-based technologies, opening up more possibilities for mobile applications. While the energy per bit is approximately a factor of three lower than cutting edge CMOS technology,[3] the process size of the SP-pMTJ is orders of magnitude smaller. Increasing the temperature of SP-MTJs also increases the speed of magnetization reversal rather than slowing down =like semiconductor RNGs.[12] As the magnetic volume of the SP-pMTJs decreases, the speed of magnetization reversal should increase exponentially. Assuming all other parameters remain constant, a 7 nm diameter MTJ would produce random bits at over 80 MHz at -800 mV. With a constant resistance-area product, such a small MTJ would have a resistance over 100 MΩ and thus reduce power consumption by an order of magnitude. Further, these types of devices can be used in probabilistic computing if the magnetoresistance can be controlled by a current or voltage.

ACKNOWLEDGMENTS

This work was supported in part by C-SPIN, one of the six centers of STARnet, a Semiconductor Research Corporation program, sponsored by MARCO and DARPA under contract no 2013-MA-2831 and by NSF grant ECCS-1709845.

[1] B. Jun and P. Kocher, "The intel random number generator," Cryptography Research Inc. white paper. (1999).
[2] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, IEEE Trans. Comput. **52**, 403 (2003).
[3] S. G. Bae, Y. Kim, Y. Park, and C. Kim, IEEE J. Solid-State Circuits **52**, 605 (2017).
[4] S. K. Piotrowski, M. F. Matty, and S. A. Majetich, IEEE Trans. Magn. **50**, 18 (2014).
[5] D. Vodenicarevic, N. Locatelli, A. Mizrahi, J. S. Friedman, A. F. Vincent, M. Romera, A. Fukushima, K. Yakushiji, H. Kubota, S. Yuasa, and S. Tiwari, arXiv preprint arXiv:1706.05262 (2017).
[6] H. Lee, F. Ebrahimi, P. K. Amiri, and K. L. Wang, AIP Advances **7**(5), 055934 (2017).
[7] M. Gajek, J. J. Nowak, J. Z. Sun, P. L. Trouilloud, E. J. O'Sullivan, D. W. Abraham, M. C. Gaidis, G. Hu, S. Brown, Y. Zhu, R. P. Robertazzi, W. J. Gallagher, and D. C. Worledge, Appl. Phys. Lett. **100**, 132408 (2012).
[8] N. Nishimura, T. Hirai, A. Koganei, T. Ikeda, K. Okano, Y. Sekiguchi, and Y. Osada, J. Appl. Phys. **91**, 5246 (2002).
[9] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "NIST special publication 800-22 revision 1a: A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST, US Department of Commerce, USA (2010).
[10] M. Bapna, S. K. Piotrowski, S. D. Oberdick, M. Li, C. L. Chien, and S. A. Majetich, Appl. Phys. Lett. **108** (2016).
[11] J. Soto, ACM SIGSIM Simul. Dig. **8**, 85 (1976).
[12] Y. Cai, Z. Cheng, Z. Yang, C. W. Tang, K. M. Lau, and K. J. Chen, IEEE Electron Device Lett. **28**, 328 (2007).