Hindawi Publishing Corporation
Advances in Condensed Matter Physics
Volume 2015, Article ID 251819, 8 pages
http://dx.doi.org/10.1155/2015/251819

Research Article

High-Density Physical Random Number Generator Using Spin Signals in Multidomain Ferromagnetic Layer

Sungwoo Chun,[1] Seung-Beck Lee,[1] Masahiko Hara,[2] Wanjun Park,[1] and Song-Ju Kim[3]

[1]*Department of Electronic Engineering, Hanyang University, Seoul 133-791, Republic of Korea*
[2]*Department Electronic Chemistry, Interdisciplinary Graduate School of Science and Engineering, Tokyo Institute of Technology, 4259 Nagatsuta, Midori-ku, Yokohama 226-8503, Japan*
[3]*WPI Center for Materials Nanoarchitectonics, National Institute for Materials Science, 1-1 Namiki, Tsukuba, Ibaraki 305-0044, Japan*

Correspondence should be addressed to Song-Ju Kim; kim.songju@nims.go.jp

Received 23 November 2014; Accepted 21 January 2015

Academic Editor: Rosa Lukaszew

Copyright © 2015 Sungwoo Chun et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

A high-density random number generator (RNG) based on spin signals in a multidomain ferromagnetic layer in a magnetic tunnel junction (MTJ) is proposed and fabricated. Unlike conventional spin-based RNGs, the proposed method does not require one to control an applied current, leading to a time delay in the system. RNG demonstrations are performed at room temperature. The randomness of the bit sequences generated by the proposed RNG is verified using the FIPS 140-2 statistical test suite provided by the NIST. The test results validate the effectiveness of the proposed RNGs. Our results suggest that we can obtain high-density, ultrafast RNGs if we can achieve high integration on the chip.

1. Introduction

High-quality random bits are desperately required in security systems, information and communication systems, and computer simulations. Although many true random number generators (RNGs) have been proposed thus far, their bit sequences occasionally include unexpected nonrandom factors, in most cases caused by the external environment. Therefore, pseudo-RNGs such as the Blum-Blum-Shub algorithm [1], the Mersenne-Twister algorithm [2], and cellular automaton [3, 4] are widely used instead. These methods easily generate bit sequences without the need for any electric or optical devices other than a computer for executing the program. The bit sequences obtained, however, are intrinsically deterministic; they are not true random sequences.

Recently, high-quality true RNGs using physical phenomena have been proposed in the fields of semiconductor laser chaos [5–7], quantum effects [8, 9], and spin devices [10, 11]. Uchida et al. [5] reported a fast RNG above the GHz region based on the phenomenon of oscillation at high frequencies generating optical turbulence in high-bandwidth chaotic semiconductor lasers. This method suggests the potential to generate high-speed random bits at up to 10 Gbps. However, their device utilizes complicated optical systems and external optical feedback with the conversion of the optical signal to an electrical signal via photodetectors.

Spintronics, an emerging technology exploiting both the intrinsic spin of the electron and its associated magnetic moment, has been researched for applications to magnetic random access memory (MRAM) [12, 13], hard disk drives [14, 15], and logic devices [16]. In particular, in the magnetic tunnel junction (MTJ) devices used in MRAM, one magnetic layer (lower) has its own magnetization orientation pinned either by being thicker than the upper-layer (called the "free layer") or by being coupled to an antiferromagnetic layer on the bottom. The orientation of the magnetization of the free layer can be switched using a magnetic field or a current. Owing to the discovery of spin transfer torque (STT) based MTJs [17], which reveal that the magnetization orientation of the magnetic layer in an MTJ and the spin valve can be modulated using a spin-polarized current, the applications of spintronics have widened. In the magnetic layer, the angular momentum of the spin-polarized current can be transferred to the magnetic layer while changing its orientation.

This spin behavior can be induced by a uniform current on the collective magnetization dynamics in a ferromagnetic metal in picoseconds. Thus, the current-induced spin behavior of the MTJ is one of the most powerful methods for physically generating a true random number. Therefore, electrical devices that can utilize current-induced spin behavior should be developed. Fukushima et al. proposed an RNG using the inversion probability of magnetization for an applied current input in an MRAM device [11]. However, this device requires current initialization, which triggers the system's time delay for preparing the initial magnetization configuration.

In this study, we demonstrate true RNG based on spin behavior in a ferromagnetic layer with a magnetic multidomain structure induced by a DC current in the perpendicular MTJ pillar (30 nm, top FM) on a chip. The proposed method does not require the initialization of an applied current. The randomness is verified using the FIPS 140-2 statistical test suite. High-quality random bits are generated in a multidomain MTJ induced by hard masking using an electron beam resist and high beam supply voltage ion beam etching. Further, we show the randomness dependency on the applied DC current amplitude, which determines the degree of spin fluctuation. Finally, we suggest ultrafast RNG using a logical XOR operation between the pMTJ cells with high integration on the chip.

2. Experimental

The p-MTJ layers, deposited by UHV sputtering (ULVAC, Inc.), use TiN(500)/Ta(30)/Ru(100)/Co-Pd multilayer(52) (thicknesses in angstroms) as the bottom electrode and the free layer, CoFeB(11)/MgO(8)/CoFeB(12), as the (001)-oriented MgO tunnel barrier layer and CoFeTb(300)/Ru(100)/Ti(50) as the pinned layer and top electrode. After arrays of 30 nm, dot-pattern, 100 nm thickness hard mask were created by 80 kV electron beam lithography (Nano-Beam, nB3) in NER (propylene glycol monomethyl ether acetate compound); an ion beam etching (IBE) process was performed by tilting the rotating sample stage with a beam supply voltage of 700 V and an acceleration supply voltage of 100 V [18, 19]. After IBE, the MTJ pillar dimensions and etching characteristics were measured using a scanning electron microscope (SEM) and a high-resolution transmission electron microscope (HR-TEM). For the electrical test samples, after the MTJ pillar was formed, SiNx was deposited using low temperature (100 K) chemical vapor deposition to create the passivation layer. Then, chemical mechanical polishing was performed to expose the top of the MTJ. Finally, the top electrode was created by optical lithography followed by Cr/Au deposition and lift-off.

3. Results and Discussion

Current-induced spin dynamics are expected to arise in magnetically inhomogeneous systems containing two or more weakly coupled magnetic layers. A uniform current input can modify the collective magnetization dynamics because it alters the distribution of quasiparticles in the momentum space [20]. The multidomain structure, which can be induced by another current density, can be added to coupled domain distributions with spin fluctuation in each domain.

In general, the multidomain characteristics of an MTJ are known to be a negative influence on the MRAM cell, because switching in the memory should be operated only by the controllable current input to maintain reliability. This means that it is difficult to use multilevel devices in memory applications. However, recently, multilevel MRAM cells have been reported to improve the current density of STT memory [21–25]. In these studies, magnetic multidomain structures induced in ferromagnetic layers fabricated by imperfect lithography and etching (which induce irregularity of shape and edge pinning) are used for RNGs.

Figure 1(a) shows the MR characteristics of the pMTJ measured in air with perpendicular magnetic fields swept between −2000 and 2000 Oe, at a sample bias voltage of 50 mV. In the case of AP-to-P reversal, good switching characteristics with a single domain are shown at −580 Oe, because multidomain factors are arranged in a stable energy state, namely, in the parallel direction state in the free layer. However, multidomain switching characteristics are shown in the range from 500 to 1700 Oe in the case of P-to-AP reversal. It is noted that these domains switch at different spin-polarized inputs and form multiple resistance levels. These multiple reversible transitions are induced by the hard masking of the e-beam resist, which forms tapered sidewalls [22, 25] on the MTJ nanopillar, as shown in the inset of Figure 1(a). Further, ion milling with a large beam supply voltage (700 V) results in a magnetic multidomain structure around the ferromagnetic layer edge, as shown in the HR-TEM image in Figure 1(b). The brightness difference in the HR-TEM image indicates that the ferromagnetic layers (pinned and free layer) with central MgO tunnel barriers are damaged toward the sidewall of the pMTJ pillar. As a consequence of this geometry, the spin configuration is not uniformly polarized in the plane of the ferromagnetic film; the results are that a spatially magnetic multidomain structure is generated. The magnetic multidomain structure generated in the ferromagnetic layer is subjected to a localized spin-polarized current, which increases the density of the freedom of spin. Its state makes it possible to generate high-quality random numbers.

The scheme for generating random bit sequences using the pMTJs is shown in Figure 2. Our method exploits the spin-configuration-dependent electrical output signals by transferring the angular momentum of the spin-polarized current. DC currents are applied to the pMTJs, flowing from the pinned to the free layer, because multidomain characteristics are observed in the P-to-AP reversal, as shown in the MR curve in Figure 1(a). A constant, positive magnetic field (100 Oe) is simultaneously applied using a gauss-meter for correcting the shift field (which is believed to be caused by a dipolar interlayer coupling between the two CoFeB layers) [26]. The signal processing in our system (Figure 2) is as follows: First, electrical output signals are extracted at 20 kbps using a Keithley 2636 A sourcemeter. The output voltage signals X_i ($i = 1$–10^6) are normalized to the form

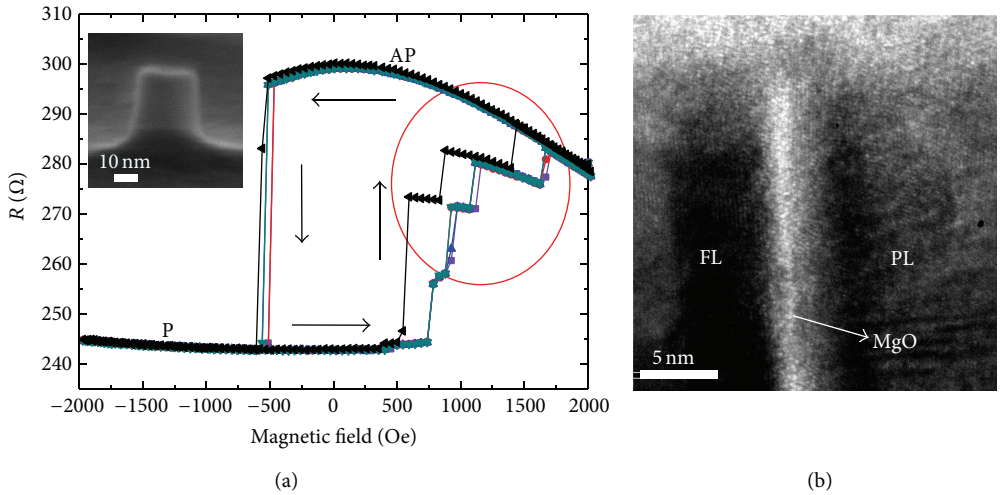


Figure 1: Multidomain properties of fabricated STT-MRAM cell. (a) MR characteristics of the pMTJ measured in air with perpendicular magnetic fields swept between −2000 and 2000 Oe, at a sample bias voltage of 50 mV. AP-to-P reversal in spin arrangement of two ferromagnetic layers is shown at the point of −580 Oe; P-to-AP reversal is shown ranging from 500 to 1700 Oe. (Inset) SEM image of individual pMTJ nanopillar with 30-nm junction. (b) High resolution transmission electron microscopy (HR-TEM) image of the pMTJ after ion milling. Brightness difference of sidewall of pinned and free layer (PL and FL) shows formation of multidomain ferromagnetic layers and damage from fabrication process, lithography, and ion milling.

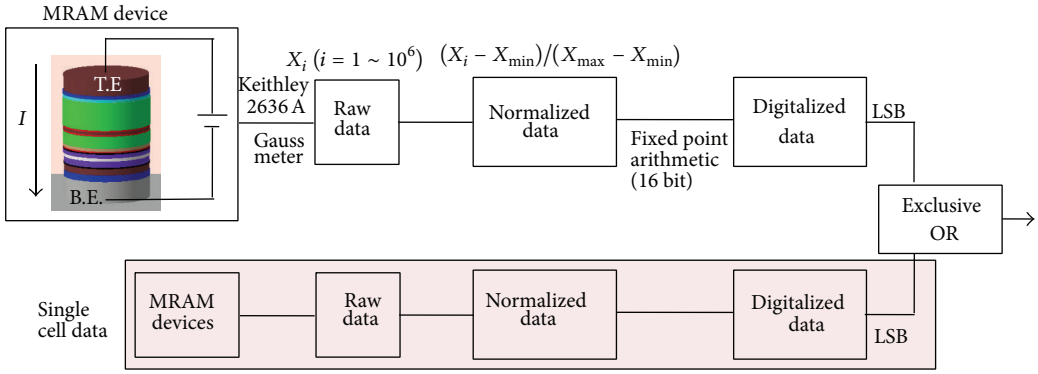


Figure 2: Schematic diagram showing scheme for generating random bit sequence using the pMTJ. The DC currents are applied to the pMTJs, flowing from the pinned to the free layer. A constant, positive magnetic field (100 Oe) is simultaneously applied by a gauss-meter to correct the shift field. Electrical output signals for spin magnetization arrangements are extracted at 20 kbps using a Keithley 2636 A sourcemeter. The output voltage signals X_i ($i = 1$–10^6) are normalized to the form $(X_i - X_{min})/(X_{max} - X_{min})$. The normalized signals are digitized using fixed-point arithmetic (16-bit). The least signification bits (LSBs) of the digitalized signal are used for binary signals. Finally, the binary signals obtained from the pMTJs are combined using an exclusive OR (XOR) method to generate a bit sequence. The single cell data method refers to data processing in only one pMTJ before the XOR operation.

$(X_i - X_{min})/(X_{max} - X_{min})$. The normalized signals are digitized using fixed-point arithmetic (16-bit). The least significant bits (LSBs) of the digitalized signal are used for binary signals. Finally, the binary signals obtained from the pMTJs are combined by an exclusive OR (XOR) gate to generate the bit sequence.

To evaluate the randomness of the spin signals obtained here, statistical tests are required. There are many well-known statistical test suites such as NIST 800-22 [27, 28], FIPS 140-2 [29], and Diehard [30]. We use the FIPS 140-2 statistical test suite because it is the simplest and most user friendly. It has only four basic tests, namely, the monobit test, the poker test, the runs test, the long run test. Additionally, instead of having the user select appropriate significance levels, for these tests, it provides explicit bounds that the computed value of a statistic must satisfy (e.g., 9725 < the number of ones in a 20000-bit sequence < 10275 for the monobit test). In fact, the FIPS 140-2 statistical test suite has been used to supplement RNGs in many hardware implementations [31–33], even though this statistical test suite stopped being supported in December 2002. Because of its simplicity, these four tests can be modified easily to evaluate any length of bit sequence. In our experiment, a 2500-bit sequence is a realistic data size for one sample, although larger data sizes are also possible, in principle. Recently, Kim et al. concluded that the FIPS 140-2 test suite does not have an identical significance

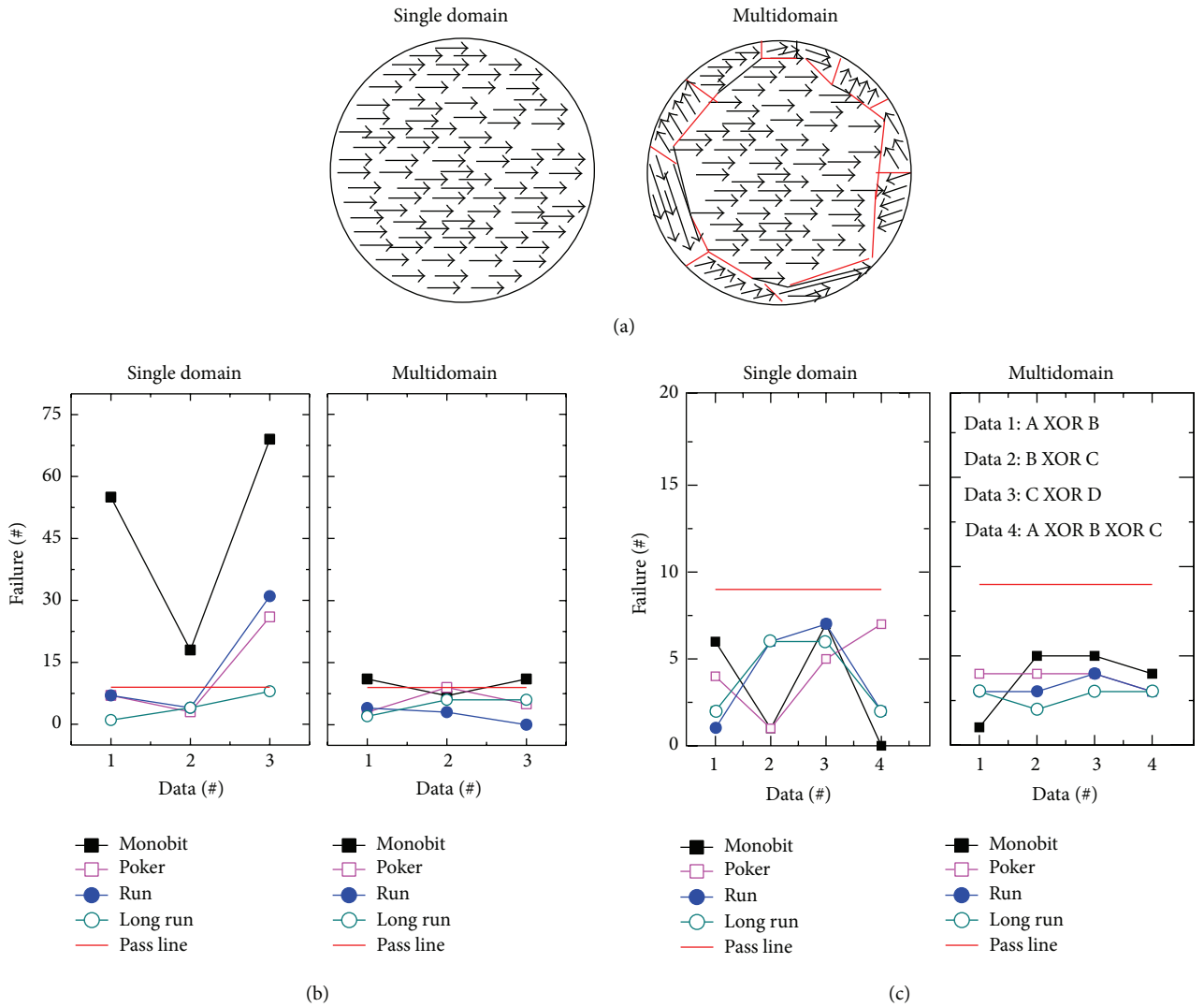


Figure 3: The randomness test for single- and multidomain pMTJ. (a) Schematic of magnetization arrangement of single- and multidomain ferromagnetic layer. The results of the randomness tests for (b) single cell data and (c) after the XOR operation. For each data set, the 2500-bit sequences are evaluated 400 times ($2500 \times 400 = 10^6$ bits). Only nine failures are acceptable for each test (point to pass line). In the multidomain data of (b), data 1 (2, 3) means XOR of digitalized data A (B, C) and B (C, A) for 10^6 bits and data 4 means the XOR of A, B, and C.

level α, [34], and correctly recalculated the requirement of the FIPS 140-2 test suite for a 2500-bit sequence, so as to have the identical significance level, $\alpha = 10^{-2}$, which is a commonly used value in cryptography. The requirements of the improved FIPS 140-2 tests are as follow [35, 36].

(1) The monobit test:

(a) Count the number of 1s in the 2500-bit stream. Denote this quantity by X.

(b) The test is passed if $1185 < X < 1315$.

(2) The poker test:

(a) Divide the 2500-bit stream into 625 consecutive 4-bit segments. Count and store the number of occurrences of the 16 possible 4-bit values. Denote $f(i)$ as the number of each 4-bit value i, where $0 \le i \le 15$.

(b) Evaluate the following:

$$X = \left(\frac{16}{625}\right) \times \left(\sum_{i=0}^{15} [f(i)]^2\right) - 625. \quad (1)$$

The test is passed if $4.6 < X < 32.8$.

(3) The runs test:

(a) A run is defined as a maximal sequence of consecutive bits of either all zeros (0-run) or all ones (1-run) that is part of the 2500-bit stream. Count the number of runs (0-runs and 1-runs) in the 2500-bit stream. Denote this quantity by X.

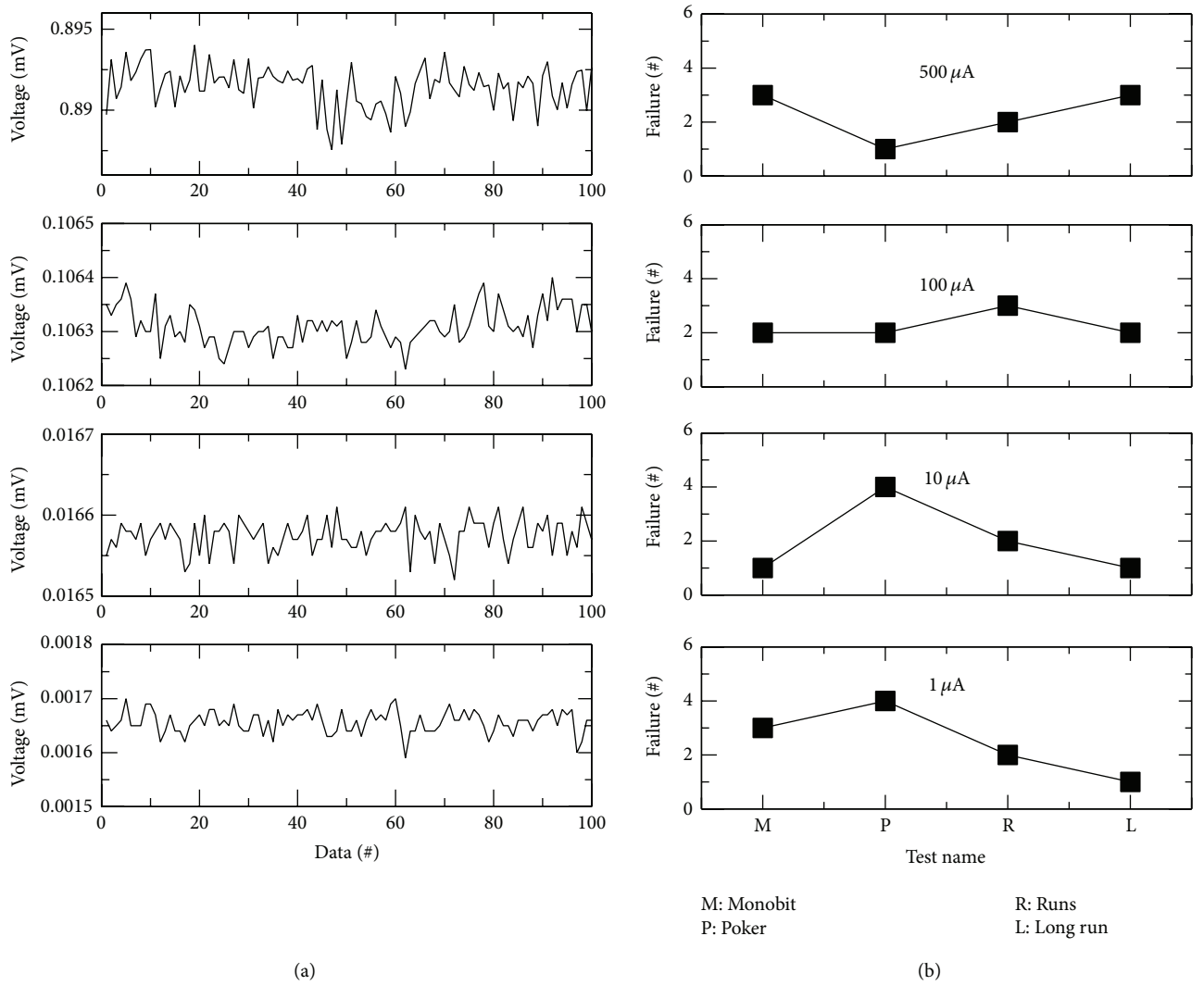


Figure 4: Randomness tests with various current amplitudes. (a) The temporal electrical output signals for the four currents (1, 10, 100, and 500 μA). (b) The evaluation of the randomness at each current level.

(b) The test is passed if $m - b \leq X \leq m + b$.

Here, $m = 5000p$, $b = 257.5828p$, $p = q(1 - q)$, and $q = (number\ of\ 1s)/2500$.

(4) The long runs test:

(a) In a sample of 2500 bits, a long run is defined as a run of length 17 or more.

(b) The test is passed if there are no long runs.

Figure 3(a) shows a schematic of the magnetization arrangement of single- and multidomain ferromagnetic layers. In a multidomain device, spins are arranged with irregular directions of magnetic domains.

Figure 3(b) shows the number of failures in the four tests of the LSB data without the logical exclusive OR operation, as shown for the single cell data method of Figure 2. The horizontal axis denotes the data set number. Every data set has 10^6 bits. For each data set, 2500-bit sequences are evaluated 400 times ($2500 \times 400 = 10^6$ bits). Only nine failures are acceptable in each test, which are shown in each graph with horizontal pass lines. All data sets fail in the case of a single domain device, whereas the multidomain data sets pass most randomness tests, except for two of the monobit tests. It is believed that the spin behavior in the magnetic multidomain structure is intrinsically more random because the spins react as a combination of domain disruption and spin fluctuations. The randomness tests also indicate that current-induced spin fluctuations can be an effective phenomenon for generating random bits.

The logical XOR operation has been used for evaluating randomness. Figure 3(c) illustrates the results of randomness test after performing the XOR operation. Data 1 (2, 3) means taking the XOR of digitalized data A (B, C) and B (C, A) for 10^6 bits and data 4 means taking the XOR of A, B, and C. The randomness tests show the generation of high-quality random numbers in both single-domain and multidomain devices, although low failure rate characteristics

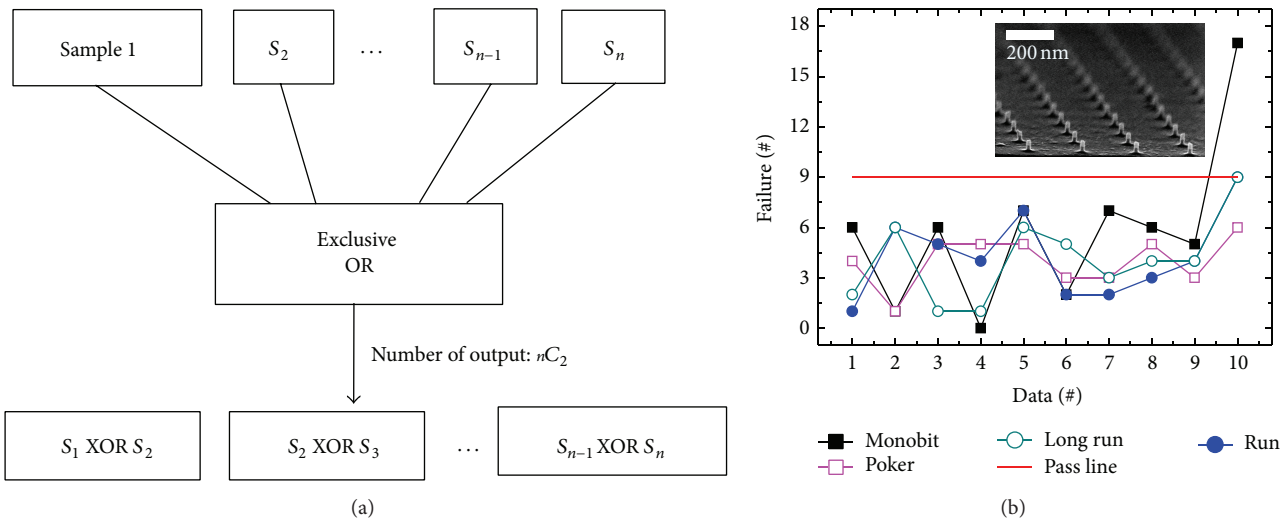


FIGURE 5: Generation of multiple random bits. (a) Schematic diagram of method for generating multiple random bits. Each signal is extracted after every XOR operation. The number of output signals follows the relation nC_2, where C is combination. (b) The evaluation of the random bits generated simultaneously in five 30 nm pMTJ pillars. The XOR data measured for five cells are 10 in number ($5C_2$); their numbers are indicated on the x-axis of the graph. (Inset) SEM image of the pMTJ array with 30 nm junction and 200 nm pitch.

in an acceptable distribution appeared only in multidomain devices.

Spin in ferromagnetic layers (the pinned layer for spin polarization and the free layer for being subjected to spin transfer torque) allows angular momentum to interact with applied spin current. Our pMTJ device has a 112 MA/cm^2 of critical current density at a resistance-area (RA) product of 10 Ω·cm^2. This means that a DC current below ~791 μA cannot induce magnetic switching in the 30 nm pillar. Figure 4 shows the results of the randomness tests for various current amplitudes. The temporal electrical output signals of the four currents (1, 10, 100, and 500 μA) on the left side of Figure 4 illustrate that high-amplitude spin fluctuation occurs at larger applied currents. However, the evaluation of randomness indicates that the quality of the random bits does not depend on the amplitude of the applied current, despite the fact that the current close to the switch free layer is applied. These results indicate that high-quality random numbers can be created at low operation biases.

pMTJ RNGs are devices that can be fabricated on chips. We can obtain synthetic random bits through integration and embed them with other, subsidiary circuits. Figure 5(a) shows a schematic diagram of the method for generating multiple random bits. Each signal is extracted at every XOR operation. The number of output signals follows the expression nC_2, where C denotes a combination. If this method is used, we can obtain ultrafast generation of random bits in the future, for example, $(7.56 \times 10^9 C_2) \times$ (20 kbps sampling) for a junction of 30 nm at a pitch of 200 nm in a 2×2 cm^2 area, as shown in the SEM image of Figure 5(b). Figure 5(b) shows the randomness evaluation of multiple random bits generated simultaneously in five 30 nm pMTJ pillars. The XOR output signals measured for five cells are 10 in number ($5C_2$); their numbers are indicated on the x-axis of the graph. Most data sets pass the four randomness tests with low failure rates. It is noted that fast random bits can be generated through the integration of nanoscale cells fabricated on the chip.

4. Conclusion

High-density RNG based on spin signals in multidomain ferromagnetic layers is proposed and a device is fabricated. RNG experiments are performed at room temperature. The degree of randomness is verified using the FIPS 140-2 statistical test suite, which is the most simple and user friendly among other conventional test suites. The test results validate the effectiveness of the proposed RNGs. In the future, we can obtain high-density, ultrafast RNGs if we achieve high integration on the chip.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was partially performed when Song-Ju Kim and Masahiko Hara were with the RIKEN Advanced Science Institute, which was reorganized and integrated into RIKEN as of the end of March 2013. The authors thank Professor Yasuhiro Ikezoe for the valuable discussions.

References

[1] L. Blum, M. Blum, and M. Shub, "A simple unpredictable pseudorandom number generator," *SIAM Journal on Computing*, vol. 15, no. 2, pp. 364–383, 1986.

[2] M. Matsumoto and T. Nishimura, "Mersenne Twister: a 623-dimensionally equidistributed uniform pseudo-random number generator," *ACM Transactions on Modeling and Computer Simulation*, vol. 8, no. 1, pp. 3–30, 1998.

[3] S. Wolfram, "Random sequence generation by cellular automata," *Advances in Applied Mathematics*, vol. 7, no. 2, pp. 123–169, 1986.

[4] S.-J. Kim and K. Umeno, "Randomness evaluation and hardware implementation of nonadditive CA-based stream cipher," *Journal of Signal Processing*, vol. 9, pp. 71–78, 2005.

[5] A. Uchida, K. Amano, M. Inoue et al., "Fast physical random bit generation with chaotic semiconductor lasers," *Nature Photonics*, vol. 2, no. 12, pp. 728–732, 2008.

[6] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, "Ultrahigh-speed random number generation based on a chaotic semiconductor laser," *Physical Review Letters*, vol. 103, no. 2, Article ID 024102, 2009.

[7] T. Harayama, S. Sunada, K. Yoshimura, P. Davis, K. Tsuzuki, and A. Uchida, "Fast nondeterministic random-bit generation using on-chip chaos lasers," *Physical Review A: Atomic, Molecular, and Optical Physics*, vol. 83, no. 3, Article ID 031803, 2011.

[8] K. Uchida, T. Tanamoto, and S. Fujita, "Single-electron random-number generator (RNG) for highly secure ubiquitous computing applications," *Solid-State Electronics*, vol. 51, no. 11-12, pp. 1552–1557, 2007.

[9] M. Naruse, S.-J. Kim, M. Aono, H. Hori, and M. Ohtsu, "Chaotic oscillation and random-number generation based on nanoscale optical-energy transfer," *Scientific Reports*, vol. 4, article 6039, 2014.

[10] T. Tanamoto, N. Shimomura, S. Ikegawa, M. Matsumoto, S. Fujita, and H. Yoda, "High-speed magnetoresistive random-access memory random number generator using error-correcting code," *Japanese Journal of Applied Physics*, vol. 50, no. 4, Article ID 04DM01, 2011.

[11] A. Fukushima, H. Kubota, K. Yakushiji, S. Yuasa, and K. Ando, "Random number generating device," the US patent (Pub. No.: US 2010/0131579 A1), 2010.

[12] C. Chappert, A. Fert, and F. N. van Dau, "The emergence of spin electronics in data storage," *Nature Materials*, vol. 6, no. 11, pp. 813–823, 2007.

[13] M. Gajek, J. J. Nowak, J. Z. Sun et al., "Spin torque switching of 20 nm magnetic tunnel junctions with perpendicular anisotropy," *Applied Physics Letters*, vol. 100, no. 13, Article ID 132408, 2012.

[14] R. Wood, "Future hard disk drive systems," *Journal of Magnetism and Magnetic Materials*, vol. 321, no. 6, pp. 555–561, 2009.

[15] S. N. Piramanayagam, "Perpendicular recording media for hard disk drives," *Journal of Applied Physics*, vol. 102, no. 1, Article ID 011301, 2007.

[16] B. Behin-Aein, D. Datta, S. Salahuddin, and S. Datta, "Proposal for an all-spin logic device with built-in memory," *Nature Nanotechnology*, vol. 5, no. 4, pp. 266–270, 2010.

[17] J. C. Slonczewski, "Current-driven excitation of magnetic multilayers," *Journal of Magnetism and Magnetic Materials*, vol. 159, no. 1-2, pp. L1–L7, 1996.

[18] S. Chun, D. Kim, J. Kwon, B. Kim, S. Choi, and S.-B. Lee, "Multi-step ion beam etching of sub-30 nm magnetic tunnel junctions for reducing leakage and MgO barrier damage," *Journal of Applied Physics*, vol. 111, no. 7, Article ID 07C722, 2012.

[19] S. Chun, D. Kim, J. Kwon, B. Kim, H. Lee, and S.-B. Lee, "Negative electron-beam resist hard mask ion beam etching process for the fabrication of nanoscale magnetic tunnel junctions," *Journal of Vacuum Science and Technology B: Microelectronics and Nanometer Structures*, vol. 30, no. 6, Article ID 06FA01, 2012.

[20] J. Fernández-Rossier, M. Braun, A. S. Núñez, and A. H. MacDonald, "Influence of a uniform current on collective magnetization dynamics in a ferromagnetic metal," *Physical Review B*, vol. 69, no. 17, Article ID 174412, 2004.

[21] O. Ozatay, N. C. Emley, P. M. Braganca et al., "Spin transfer by nonuniform current injection into a nanomagnet," *Applied Physics Letters*, vol. 88, no. 20, Article ID 202502, 2006.

[22] X. Lou, Z. Gao, D. V. Dimitrov, and M. X. Tang, "Demonstration of multilevel cell spin transfer switching in MgO magnetic tunnel junctions," *Applied Physics Letters*, vol. 93, no. 24, Article ID 242502, 2008.

[23] H. X. Wei, F. Q. Zhu, X. F. Han, Z. C. Wen, and C. L. Chien, "Current-induced multiple spin structures in 100 nm ring magnetic tunnel junctions," *Physical Review B—Condensed Matter and Materials Physics*, vol. 77, no. 22, Article ID 224432, 2008.

[24] Y. Chen, W.-F. Wong, H. Li, C.-K. Koh, Y. Zhang, and W. Wen, "On-chip caches built on multilevel spin-transfer torque RAM cells and its optimizations," *ACM Journal on Emerging Technologies in Computing Systems*, vol. 9, no. 2, article no. 16, 2013.

[25] P. M. Braganca, O. Ozatay, A. G. F. Garcia, O. J. Lee, D. C. Ralph, and R. A. Buhrman, "Enhancement in spin-torque efficiency by nonuniform spin current generated within a tapered nanopillar spin valve," *Physical Review B—Condensed Matter and Materials Physics*, vol. 77, no. 14, Article ID 144423, 2008.

[26] S. Ikeda, K. Miura, H. Yamamoto et al., "A perpendicular-anisotropy CoFeB–MgO magnetic tunnel junction," *Nature Materials*, vol. 9, no. 9, pp. 721–724, 2010.

[27] A. Ruhin, J. Soto, J. Nechvatal et al., *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, Computer Security National Institute of Standards and Technology, 2010, http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf.

[28] S.-J. Kim, K. Umeno, and A. Hasegawa, "On the NIST statistical test suite for randomness," *IEICE Technical Report*, vol. 103, no. 499, pp. 21–27, 2003, https://eprint.iacr.org/2004/018.pdf.

[29] FIPS PUB 140-2, "Security Requirements for Cryptographic Modules," U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2001, http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexd.pdf.

[30] The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness, 1995, http://stat.fsu.edu/pub/diehard/.

[31] A. Hasegawa, S.-J. Kim, and K. Umeno, "IP core of statistical test suite of FIPS 140-2," in *Proceedings of the International Workshop on IP Based SoC Design*, pp. 111–114, 2003.

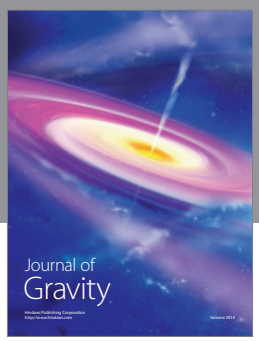
[32] R. Santoro, O. Sentieys, and S. Roy, "On-line monitoring of random number generators for embedded security," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS '09)*, pp. 3050–3053, IEEE, Taipei, Taiwan, May 2009.

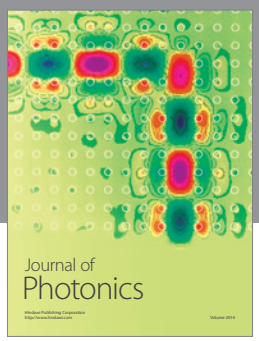
[33] J. S. Lee, P. Choi, S.-J. Kim, B.-D. Choi, and D. K. Kim, "Built-in hardware pseudo-random test module for Physical Unclonable Functions," *Nonlinear Theory and Its Applications, IEICE*, vol. 5, no. 2, pp. 101–112, 2014.

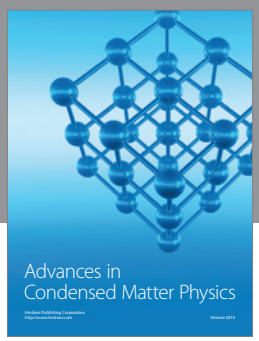
[34] S.-J. Kim, K. Umeno, and A. Hasegawa, "FIPS 140-2 statistical test suite has inappropriate significance levels," *ISM Report on Research and Education*, vol. 17, pp. 326–327, 2003.

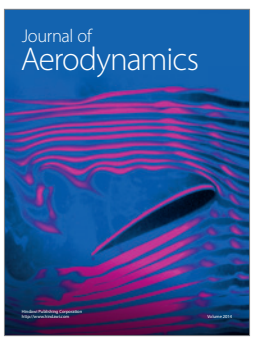
[35] Y. Ikezoe, S.-J. Kim, I. Yamashita, and M. Hara, "Random number generation by a two-dimensional crystal of protein molecules," *Langmuir*, vol. 25, no. 8, pp. 4293–4297, 2009.

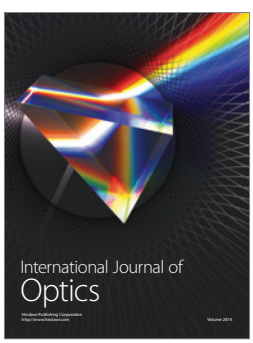
[36] Y. Ikezoe, S.-J. Kim, D. Kim, S.-B. Lee, and M. Hara, "Nanoscale shuffling in a template-assisted self-assembly of binary colloidal particles," *Journal of Nanoscience and Nanotechnology*, vol. 12, no. 3, pp. 2934–2938, 2012.

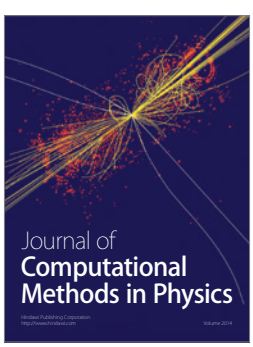


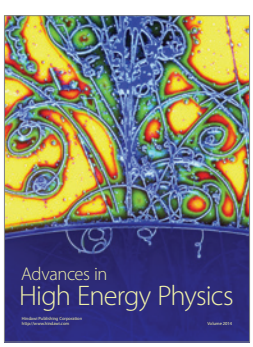


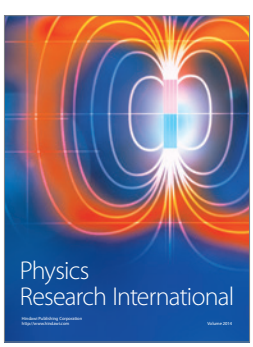


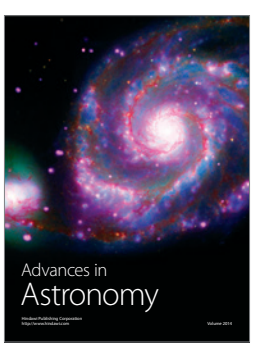


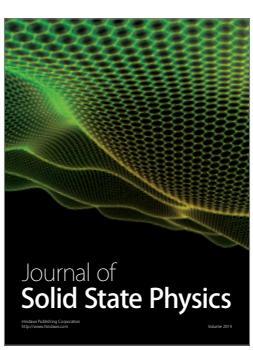


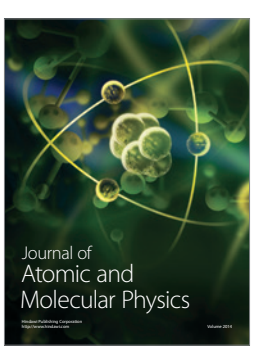












Hindawi

Submit your manuscripts at
http://www.hindawi.com