A True Random Number Generator based on Parallel STT-MTJs

Yuanzhuo Qu, Jie Han, Bruce F. Cockburn and Witold Pedrycz
Electrical and Computer Engineering
University of Alberta
Edmonton, Alberta, Canada
{yuanzhuo, jhan8, cockburn, wpedrycz}@ualberta.ca

Yue Zhang and Weisheng Zhao
Electronic and Information Engineering
Beihang University
Beijing, China
{yz, weisheng.zhao}@buaa.edu.cn

***Abstract*—Random number generators are an essential part of cryptographic systems. For the highest level of security, true random number generators (TRNG) are needed instead of pseudo-random number generators. In this paper, the stochastic behavior of the spin transfer torque magnetic tunnel junction (STT-MTJ) is utilized to produce a TRNG design. A parallel structure with multiple MTJs is proposed that minimizes device variation effects. The design is validated in a 28-nm CMOS process with Monte Carlo simulation using a compact model of the MTJ. The National Institute of Standards and Technology (NIST) statistical test suite is used to verify the randomness quality when generating encryption keys for the Transport Layer Security or Secure Sockets Layer (TLS/SSL) cryptographic protocol. This design has a generation speed of 177.8 Mbit/s, and an energy of 0.64 pJ is consumed to set up the state in one MTJ.**

***Keywords*—magnetic tunnel junctions; true random number generators; statistical tests; device variations**

I. Introduction

Data security is an increasing concern given the rapidly growing volume of valuable data being transmitted over the Internet. To ensure data security, encryption is employed to protect sensitive data such as personal or financial information. Data encryption prevents unauthorized parties from accessing the data during storage and communication.

In cryptography, a sufficiently random bit sequence is essential in an encryption algorithm. To produce random numbers, two categories of random number generators (RNGs) are used: pseudo-random number generators (PRNGs) and true random number generators (TRNGs) [1]. The sequences generated from a PRNG are fully deterministic but they have statistical properties that make them look random, so they are widely used in stochastic computing [2]. However, the predictability of PRNGs undermines the security level and thus TRNGs are sought for use in cryptography.

In contrast with PRNGs, TRNGs generate numbers with true randomness that originates from nondeterministic physical phenomena [1]. Random physical events, such as the chaotic behavior in semiconductor lasers, can produce random bits extremely fast (480 Gbit/s is reported in [3]). However, major drawbacks exist in scalability and compatibility with CMOS technology. All-digital TRNGs using metastability [4] and oscillator jitter [5] tend to have relatively poor randomness, so careful calibration or post-processing is usually needed, which increases the area and energy. In contrast, TRNGs based on device noise, such as oxide breakdown, can produce high-quality random numbers, but they have a relatively slow generation speed (e.g., only 11 kbit/s in [6]).

Therefore we seek a TRNG that can produce random sequences for cryptographic applications with high statistical quality, high speed and CMOS compatibility. Magnetic tunnel junctions (MTJs) with spin transfer torque (STT) switching are used in the proposed design by leveraging their controllable intrinsic stochastic behaviors. STT-MTJs have the advantages of high density, high endurance, and CMOS compatibility [7].

Due to fabrication limitations, resistance variations exist in MTJs. The variations affect the current through devices, which will lead to a probability bias in the generated sequences. If only one MTJ is used, the resulting bias is unacceptably large for TRNG applications. To minimize the variation effect, a parallel structure with multiple MTJs is proposed. Simulation results for various numbers of parallel MTJs show that the probability bias due to variations becomes negligible when at least 16 MTJs are used together. Moreover, the parallel structure also results in faster bit generation than using a single MTJ.

The proposed design was verified in simulation using the perpendicular magnetic anisotropy (PMA) STT-MTJ compact model with ST Microelectronics' 28-nm fully depleted silicon-on-insulator (FD-SOI) CMOS technology. Transient and Monte Carlo (MC) simulations show that the proposed TRNG can produce random bits at 177.8 Mbit/s, while consuming 0.64 pJ per generated bit. The randomness quality was validated using the National Institute of Standards and Technology (NIST) SP-800 statistical test suite.

The rest of the paper is organized as follows. Section II provides background on the MTJ device and on stochastic STT switching. Section III discusses the switching probability problems for one MTJ. The proposed design and generation procedures are presented in Section IV. Section V evaluates the simulation results and conclusions are drawn in Section VI.

II. Preliminaries

A. MTJ device structure

An MTJ is a basic spintronic device that exploits the effects of tunnel magnetoresistance. Fig. 1 shows a typical structure of the MTJ, which has a sandwich structure with three layers: two

978-3-9815370-8-6/17/$31.00 ©2017 IEEE

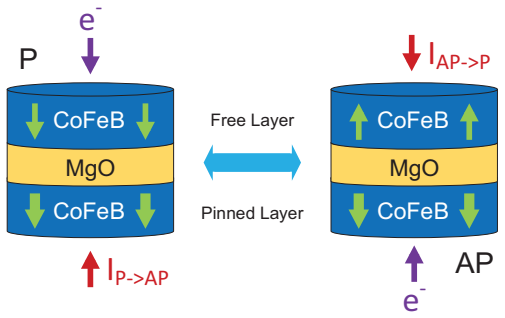

Fig. 1. The structure of an MTJ and the switching between two states.

relatively thick ferromagnetic layers (e.g. CoFeB) separated by one relatively thin tunneling barrier layer (e.g. MgO). One of the ferromagnetic layers is called the free layer for its switchable magnetization and the other one is called the pinned layer or fixed layer for its fixed magnetization. There are two stable states for an MTJ, parallel (P) or anti-parallel (AP), determined by the relative magnetization of the two ferromagnetic layers. The device has a lower electrical resistance R_P in the P state and a higher resistance R_{AP} in the AP state. The tunnel magnetoresistance ratio (TMR) = $(R_{AP} - R_P) / R_P$ characterizes the relative resistance difference between the two states, which is typically between 150% and 200% [7].

B. MTJ parameter variations

The two resistance values R_P and R_{AP} are affected by several factors such as the dimensions of the MTJ as well as other material properties. To consider this effect at the design stage, three parameters are extracted to represent the MTJ variations: the thickness of the tunneling barrier layer (t_{ox}), the thickness of the free layer (t_{sl}) and the TMR value. These parameters are assumed to follow Gaussian distributions with standard deviations of 3% of the expected values [8]. The resistance is affected by the combined effects of these parameters.

The distributions of the two resistance values for the MTJ model used in the design are shown in Fig. 2. The mean values of R_P and R_{AP} are 8.1 kΩ and 23.7 kΩ, respectively, and the standard deviation is 6.3% of the mean. In a TRNG design, MTJ variations will affect the current in circuits and these variations can undermine the quality of the generated random numbers.

C. MTJ probabilistic switching

To set the state of an MTJ, a current is injected into the MTJ from one direction to produce an effect called spin transfer torque (STT) switching. If the current is injected from the pinned layer side, the MTJ will be set to the AP state. If the current is from the free layer side, the MTJ will be set to the P state (Fig. 1) [7].

However, due to thermal fluctuations of magnetization during STT switching, the time to complete the switching follows a statistical distribution. The switching is probabilistic given a fixed current and pulse duration. The relationship between the amplitude (I), duration (t) of the current pulse and the switching probability (P) can be expressed as follows:

$$P(I,t) = 1 - \exp\left\{-\frac{t}{\tau_0}\exp\left[-\Delta\left(1-\frac{I}{I_{c0}}\right)^2\right]\right\}, \qquad (1)$$

where τ_0 is the attempt time, I_{c0} is the critical switching current

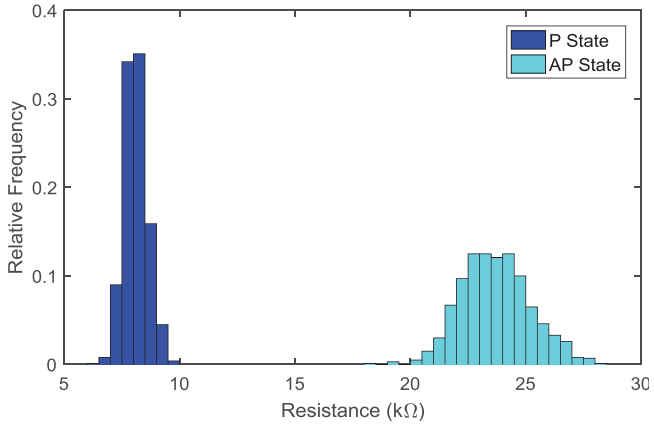

Fig. 2. The resistance distributions of R_P and R_{AP} in 28-nm PMA-STT-MTJ. 1000 Monte Carlo simulations were performed for each resistance state.

at 0 K and Δ is the thermal stability factor related to temperature, which can be seen as a fitting parameter [9].

III. Single MTJ Switching

Based on (1), when the current (I) and the pulse duration (t) are well controlled, a certain switching probability for an MTJ can be achieved. An MTJ will be in either state with equal probability after a carefully controlled current pulse aiming for 50% switching probability is applied. Then a random bit will be output by sensing the state of the MTJ. This intrinsic stochastic behavior is exploited to generate random numbers.

The switching probability of a single MTJ under different voltages, pulse durations and process corners was simulated by means of Monte Carlo simulations. A PMA-STT-MTJ compact model [10] was used with 28-nm FD-SOI CMOS technology, and the hybrid MTJ/CMOS circuits were simulated in Cadence Virtuoso. The values of the parameters used in the MTJ model are listed in Table I; other parameters retain the default values given in [10].

Single MTJ switching probabilities under different voltages with 5-ns and 10-ns pulse durations are shown in Fig. 3. The switching current is applied from a voltage source (V_{write}) and controlled by two access NMOS transistors (inset of Fig. 3). Considering speed, 5-ns pulse durations are chosen to generate the random numbers for faster operation. Further, considering power consumption, the initial state of MTJ is set to the P state to reduce voltage and to save energy. Under these conditions, more simulations are done at around 50% switching probability to determine the precise voltage needed. Using a parameter sweeping method in the MC simulation, a voltage of 1.52 V for V_{write} was finally chosen from the results of 1000 simulations.

TABLE I
MTJ Parameters [10]

Parameter	Description	Value
M_S	Saturation Field in the Free Layer	$1257 \times 10^3\ A/m$
t_{ox}	Thickness of the MgO layer	0.85 nm
$\sigma_{t_{ox}}$	Standard deviation of t_{ox}	3% of 0.85 nm
t_{sl}	Thickness of the free layer	1.3 nm
$\sigma_{t_{sl}}$	Standard deviation of t_{sl}	3% of 1.3 nm
TMR	Tunnel magnetoresistance ratio	200%
σ_{TMR}	Standard deviation of TMR	3% of 200%
$Area$	MTJ dimensions	28 nm × 28 nm × π/4

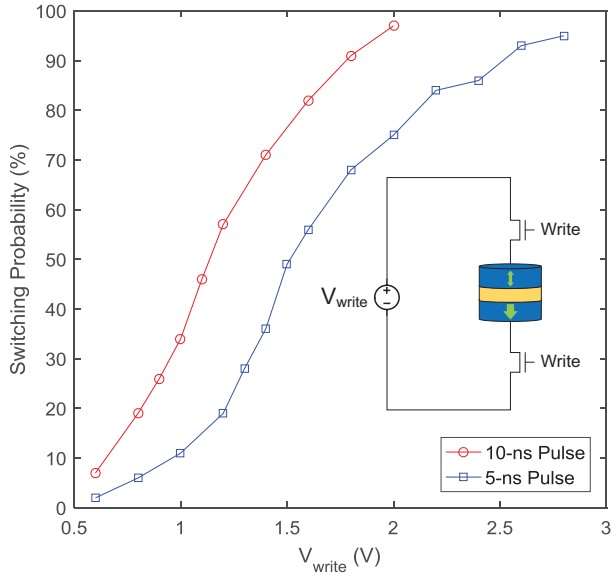

Fig. 3. The switching probability under different voltages with 5-ns and 10-ns pulse durations. The initial state is the P state. Each result is an average from 100 Monte Carlo simulations.

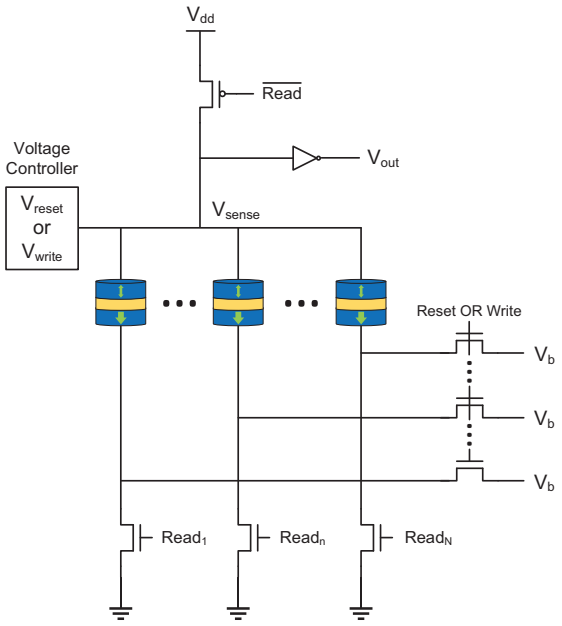

Fig. 4. Proposed TRNG with multiple parallel MTJs.

Since parameter variations exist in all MTJs, the resistance of any particular MTJ will differ a little from the expected value. Therefore, the current going through it differs and so does the switching probability, which will lead to a probability bias in the generated sequences. The MTJ variation at the initial P state will lead to a standard deviation of 3.14% in the actual probability from the ideal 50%. Therefore, using only one MTJ is not sufficient to generate practical random sequences because the probability varies from 40.58% to 59.42% over $\pm 3\sigma$. Other methods are required to improve the randomness quality.

IV. Proposed TRNG based on STT-MTJs

The proposed parallel MTJ circuit can compensate for the variation problem without the use of complicated circuits. Since the standard deviation of the average of N independent Gaussian-distributed random variables is

$$\sigma_{\frac{X_1+\cdots+X_N}{N}} = \frac{\sqrt{\sigma_1^2+\cdots+\sigma_N^2}}{N} \left(= \frac{\sigma_N}{\sqrt{N}},\ if\ X_1 = \cdots = X_N\right), \quad (2)$$

the random sequences generated by multiple MTJs will have smaller standard deviations (divided by $\sqrt{N}$) in the probability. In other words, the parallel structure averages the biased probabilities of each single MTJ to get an overall probability closer to 50%.

Based on the stochastic switching mechanism of the STT-MTJs and some similar TRNG designs with other devices [11], the schematic for the proposed TRNG was designed as shown in Fig. 4. Three MTJs are shown in the figure, but the actual number N of MTJs used can be adjusted according to the requirements.

For an array with N MTJs, the control signals are *Reset, Write* and $Read_n$ $(n = 1, 2, \cdots, N)$. To produce random numbers, the circuit needs to go through $N + 2$ phases: 1) a reset phase, 2) a write phase and 3) N read phases, with each phase taking 5 ns. In each phase, the corresponding control signal is high while the others are low. In the first two phases, all MTJs work simultaneously. In the read phases, one MTJ is sensed at a time. Here the $N + 2$ phases are explained in detail:

1) Group Reset: In the reset phase, the voltage controller drives V_{reset}, and current flows from the free layer (top) to the pinned layer (bottom) until all MTJs are switched to the P state. V_{reset} is higher enough than V_b to ensure an almost deterministic switching to the P state. At the end of the reset phase, all MTJs are in the P state waiting for the write phase.

2) Group Write: In the write phase, the voltage controller drives V_{write}, which is lower than V_b to induce a switching current going from the pinned layer to the free layer. Since the MTJs are connected in parallel, the voltages across each MTJ and the corresponding transistors are the same. All MTJs are written simultaneously, but each MTJ switches independently without affecting any other. At the end of the write phase, an MTJ will change to the AP state if it switches; otherwise, it will remain in the P state.

3) Read: In the read phases, the current flows from V_{dd} to GND passing through only the selected MTJ. Depending on the resistance of that MTJ, the V_{sense} will differ (the voltage controller is off). The inverter (or some other kind of sense amplifier) will detect the difference and amplify it. Finally, the digital output at V_{out} will indicate the resistance state of the selected MTJ.

The proposed parallel structure will not only produce random numbers with higher quality but also introduce other advantages compared with a single MTJ circuit. First, only one multiplexed sensing circuit is needed to read out all states of the N MTJs at V_{out}, which saves hardware. Also, all MTJs are reset and written simultaneously, which requires less time compared with using a single MTJ to obtain the same number of random bits. Since $(N + 2) \times 5$ ns are needed to produce N random bits, a generation speed of $\frac{N}{N+2} \times 200$ Mbit/s can be achieved. If N is large enough, the read phase will dominate the operation speed and the speed will converge to ~200 Mbit/s.

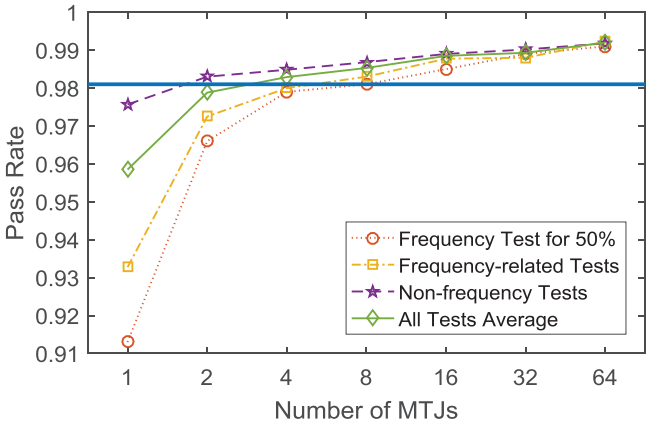

Fig. 5. Statistical quality pass rates of the proposed MTJ-based TRNGs.

V. Evaluation

In cryptography applications, such as Internet security, the typical key length is 256 bits for a Transport Layer Security or Secure Sockets Layer (TLS/SSL) cryptographic protocol [12]. Therefore, 256-bit sequences were generated using the proposed TRNG for a variety of N values.

For each N value, the proposed generation procedure was repeated $\frac{256}{N}$ times, and each MTJ was used $\frac{256}{N}$ times to generate $\frac{256}{N}$ random bits, where N is the number of MTJs in the array. After one sequence of 256 bits is generated, a new set of N MTJs is used to generate the next sequence. Altogether 1000 sequences were generated for each N value.

It is important to note that the statistical quality of most previous TRNG designs based on STT-MTJs was demonstrated only by showing that the generation has a probability of 50% [13], without mentioning other properties [14]. The quality of the random sequences needs to be evaluated in aspects other than frequency to prove the practical functionality of the proposed TRNG. Therefore, we applied the widely used statistical test suite NIST Special Publication 800-22 rev.1a [15]. Four frequency-related tests and six non-frequency-related tests were selected to examine whether a sequence has a good randomness quality in terms of frequency and other important aspects. Other tests in the suite were not chosen because they require millions of bits in a sequence.

Fig. 5 shows the result of the pass rates. According to the settings in the test suite, the threshold for passing the tests is 0.981 (the bold horizontal line in Fig. 5). The four curves illustrate the increasing quality of the generators for different categories of tests with the increasing number of MTJs used. It is shown that when only one MTJ is used, the results fall far below the standard. However, using at least 16 MTJs makes the pass rate for all tests no less than 0.981, which means that the generators can pass all 10 randomness tests.

TABLE II
Performance Comparisons

	[13]	Proposed Design (with 16 MTJs)
Technology	90 nm	28 nm
Frequency	66.7 MHz	177.8 MHz
Area Estimation	Not reported	7.64 μm^2
Energy	Not reported	0.64 pJ/bit
Statistical Tests	Not reported	Passed

The hardware simulation results are summarized in Table II and are compared with those in [13]. Since various sensing circuits can be used and the read phases consume the least energy, the reported energy excludes the read phases.

VI. Conclusions

A true random number generator based on multiple MTJs is proposed. The intrinsic stochastic behavior of STT-MTJs is exploited and a parallel structure is implemented to minimize the effects of device variations. Monte Carlo simulations are performed to verify the functionality of the proposed design. Evaluations show that device variation effects are significantly reduced by the parallel structure. The NIST statistical test suite validates the statistical quality of the generated 256-bit random sequences. This design is also energy-efficient (0.64 pJ/bit) with a high generation speed (177.8 MHz).

References

[1] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. CRC Press, Boca Raton, FL, 1997.

[2] J. Han, H. Chen, J. Liang, P. Zhu, Z. Yang and F. Lombardi, "A Stochastic Computational Approach for Accurate and Efficient Reliability Evaluation," *IEEE Trans. Computers*, vol. 63, no. 6, pp. 1336-1350, 2014.

[3] N. Oliver, M. Soriano, D. Sukow and I. Fischer, "Fast Random Bit Generation Using a Chaotic Laser: Approaching the Information Theoretic Limit," *IEEE J. Quantum Electronics*, vol. 49, no. 11, pp. 910-918, 2013.

[4] S. Mathew, S. Srinivasan, M. Anders, H. Kaul, S. Hsu, F. Sheikh, A. Agarwal, S. Satpathy and R. Krishnamurthy, "2.4 Gbps, 7 mW All-Digital PVT-Variation Tolerant True Random Number Generator for 45 nm CMOS High-Performance Microprocessors," *IEEE J. Solid-State Circuits*, vol. 47, no. 11, pp. 2807-2821, 2012.

[5] 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 smartcard IC," *IEEE Trans. Computers*, vol. 52, no. 4, pp. 403-409, 2003.

[6] N. Liu, N. Pinckney, S. Hanson, D. Sylvester and D. Blaauw, "A true random number generator using time-dependent dielectric breakdown," *IEEE Symp. VLSI Circuits*, pp. 203-204, 2010.

[7] W. Kang, Z. Li, J. Klein, Y. Chen, Y. Zhang, D. Ravelosona, C. Chappert and W. Zhao, "Variation-Tolerant and Disturbance-Free Sensing Circuit for Deep Nanometer STT-MRAM," *IEEE Trans. Nanotechnology*, vol. 13, no. 6, pp. 1088-1092, 2014.

[8] N. Rizzo, F. B. Mancoff, R. Whig, K. Smith, K. Nagel, T. Andre, P. G. Mather, S. Aggarwal, J. M. Slaughter, D. Mitchell, and S. Tehrani, "Toggle and spin torque: MRAM at Everspin Technologies," *Proc. Non-Volatile Memories Workshop*, 2010

[9] A. Fukushima, T. Seki, K. Yakushiji, H. Kubota, H. Imamura, S. Yuasa and K. Ando, "Spin dice: A scalable truly random number generator based on spintronics," *Appl. Phys. Express*, vol. 7, no. 8, p. 083001, 2014.

[10] Y. Zhang, W. Zhao, Y. Lakys, J. Klein, J. Kim, D. Ravelosona and C. Chappert, "Compact Modeling of Perpendicular-Anisotropy CoFeB/MgO Magnetic Tunnel Junctions," *IEEE Trans. Electron Devices*, vol. 59, no. 3, pp. 819-826, 2012.

[11] P. Knag, W. Lu and Z. Zhang, "A Native Stochastic Computing Architecture Enabled by Memristors," *IEEE Trans. Nanotechnology*, vol. 13, no. 2, pp. 283-293, 2014.

[12] T. Dierks, "The transport layer security (TLS) protocol version 1.2," 2008. [Online]. Available: http://tools.ietf.org/html/rfc5246

[13] S. Oosawa, T. Konishi, N. Onizawa and T. Hanyu, "Design of an STT-MTJ based true random number generator using digitally controlled probability-locked loop," *2015 IEEE 13th International New Circuits and Systems Conference (NEWCAS)*, 2015.

[14] Y. Wang, H. Cai, L. A. B. Naviner, J. O. Klein, J. Yang and W. Zhao, "A novel circuit design of true random number generator using magnetic tunnel junction," *2016 IEEE/ACM International Symposium on Nanoscale Architectures (NANOARCH)*, 2016.

[15] National Institute of Standards and Technology, Special Publication 800-22 rev.1a, 2010. [Online]. Available: http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html