STT-ANGIE: Asynchronous True Random Number GEnerator Using STT-MTJ

Ben Perach and Shahar Kvatinsky
Viterbi Faculty of Electrical Engineering, Technion - Israel Institute of Technology, Haifa, Israel
benperach@campus.technion.ac.il shahar@ee.technion.ac.il

***Abstract*—The Spin Transfer Torque Magnetic Tunnel Junction (STT-MTJ) is an emerging memory technology whose interesting stochastic behavior might benefit security applications. In this paper, we leverage this stochastic behavior to construct a true random number generator (TRNG), the basic module in the process of encryption key generation. Our proposed TRNG operates asynchronously and thus can use small and fast STT MTJ devices. As such, it can be embedded in low-power and low-frequency devices without loss of entropy. We evaluate the proposed TRNG using a numerical simulation, solving the Landau–Lifshitz–Gilbert (LLG) equation system of the STT-MTJ devices. Design considerations, attack analysis, and process variation are discussed and evaluated. The evaluation shows that our solution is robust to process variation, achieving a Shannon-entropy generating rate between 99.7Mbps and 127.8Mbps for 90% of the instances.**

***Index Terms*—TRNG, security, memristors, STT-MTJ, MRAM**

I. Introduction

In cryptography, the encryption algorithm is generally assumed to be known to the adversary and the only secret is the encryption key. Without this key, it should not be possible to decrypt the data. The key should therefore be generated by a random process, making it improbable to guess. Such processes are called *Random Number Generators* (RNGs). One class of RNGs are *True Random Number Generators* (TRNGs). A TRNG is based on a truly random physical process, making this approach attractive since the random numbers can only be guessed from the process distribution.

With the rising concern for security, many devices will need to use encryption and generate keys in some manner; hence, every such device will need an RNG of its own. To this end, a truly random physical mechanism with low power, low area, and a high generating rate is desired. One such mechanism can be the switching time of the STT-MTJ (Spin Transfer Torque Magnetic Tunnel Junction) device. STT-MTJ (or STT-MRAM) has relatively low operating energy and low area, and its switching time stochasticity has been thoroughly established.

Prior work has proposed TRNGs based on STT-MTJ devices [1]–[3]. These works use a current pulse on an MTJ device to achieve a switching probability of 50%. The pulse needs to be controlled by a feedback circuit due to process variation and environmental changes. The feedback circuit requires a clock, further complicating and binding the system.

In this paper, we propose STT-ANGIE, an asynchronous TRNG based on STT-MTJ devices. Since the randomness extraction is independent of the system clock, our TRNG can be embedded in low-frequency devices without decreasing randomness. We numerically simulate the behavior of our TRNG using stochastic physical modeling of the STT-MTJ and show that it is robust to process variation and environmental conditions. To the best of our knowledge, this is the first work on a TRNG using STT-MTJ that includes analysis of attacks that might be carried out by an adversary. Such analysis, essential for a security system, was conducted only on other security devices incorporating STT-MTJs [4].

II. Background

A. True Random Number Generators

TRNG is a source of random numbers with some output distribution, not necessarily uniform. A TRNG output might go through post-processing before it is used, even if its output distribution is uniform. In the literature, these post-processing methods are referred to as *randomness extractors* [5]. Randomness extractors aim to compensate for the non-uniformity of the TRNG and other real-world effects, such as process variation, wear-out of the components and outer interference, all of which will change the distribution and might reduce the randomness of the TRNG. Hence, it is common to use such an extractor. If an extractor is used, the TRNG itself does not need to have a uniform distribution to qualify for cryptographic use. However, the closer the TRNG output distribution is to uniform, the simpler the extractor can be.

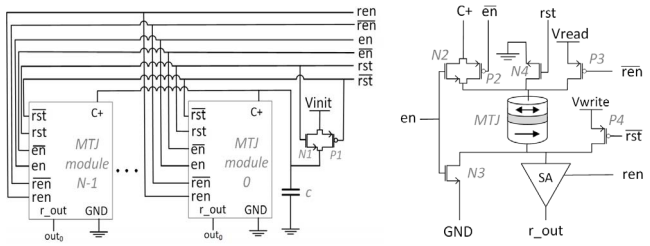
Additional important properties of TRNGs are robustness to process and environmental variations and a high generating rate. An attacker may try to change the environmental parameters (*e.g.*, electromagnetic field) to decrease the randomness of the TRNG. To ensure the proper functioning of a TRNG, statistical tests are usually performed on its output before the randomness extractor. Those tests, referred to as *online tests*, are run during the operation of the TRNG.

B. STT-MTJ Devices

An STT-MTJ is structured as two ferromagnetic layers separated by a tunnel barrier layer [6], [7]. One ferromagnetic layer has a fixed magnetization direction. The other layer can switch its magnetization direction, parallel (P) or anti-parallel (AP) to the direction of the fixed layer, when current is driven through the device. The current direction determines the direction of the switch. When there is no current, the free layer will tend to remain in either of the stable states, P or AP, but might randomly switch between them due to thermal fluctuations [6]. In this paper, in-plane MTJs are used, where the magnetization direction of the ferromagnetic layers is in the plane of the layers.

The resistance of the MTJ depends on its state and is marked as R_{on} and R_{off} for the P and AP states respectively, where

978-3-9819263-2-3/DATE19/©2019 EDAA



(a) (b)

Fig. 1. The proposed TRNG consists of (a) N parallel connected MTJ-modules and a capacitor. (b) Schematic of the MTJ module.

$R_{on} < R_{off}$. By applying a low voltage on an MTJ and sensing the current, the state of the MTJ can be determined.

To physically model the dynamics of the STT-MTJ device, an approximation of the magnetization of the free layer as a single domain is typically used. The dynamics of the magnetization are well described by the phenomenological Landau-Lifshitz-Gilbert (LLG) equation [8], with the addition of a stochastic term for the thermal fluctuations [9] and Slonczewski's STT term [10].

III. TRNG Structure and Operation

The proposed TRNG generates N-bit numbers and is composed of a capacitor, N STT-MTJ devices, N sense amplifiers, and transistors that serve as switches, as shown in Figure 1.

The TRNG operation consists of three steps, each operating in a fixed amount of time. The first step, the *Reset* step, charges the capacitor C to the V_{init} voltage (using transistors $N1$ and $P1$) and applies a current through the MTJ devices (using transistors $N4$ and $P4$), switching them to the AP state. The second step, the *Enable* step, connects C in parallel to all the MTJ devices (using transistors $N2, N3$, and $P2$). This discharges C through the MTJ devices, enabling them to switch to the P state with some probability. The third step, the *Read* step, applies a small current through the MTJ devices (using transistor $P3$), and the sense amplifiers determine the state of each. The AP/P states are interpreted as '0'/'1' respectively. Overall, the TRNG outputs an N-bit word.

The proposed TRNG randomness is based on the stochastic switching time of the MTJ. Unlike previously proposed TRNGs, the randomness extraction operation in the Enable step is asynchronous and does not depend on a strict time measurement. The capacitor is sufficiently discharged during the Enable step to ensure a low probability for further switching. During the Enable step, the resistance of an MTJ drops if it is switched, making the capacitor discharge faster. This lowers but does not eliminate the switching probability of the other MTJs.

IV. Evaluation

A. Measure for Randomness

We use two measures to evaluate the randomness of our TRNG: the Shannon entropy and the min-entropy. For an i.i.d. process with values from a finite set $\mathcal{X}$ with probability p, the Shannon entropy per word is $-\sum_{x\in\mathcal{X}} p(x)log_2p(x)$ and the min-entropy per word is $\min_{x\in\mathcal{X}}(-log_2p(x))$. Both entropies are measured in bits. Since a simulated model is used, standard statistical tests are irrelevant.

The min-entropy is the lowest amount of randomness a single sample of a random variable can give. Randomness extractors are sometimes designed to extract an output for every input, so the correct measure here is the min-entropy of their source [5]. The Shannon entropy is the expected randomness from a random variable. For an i.i.d. source, the Shannon entropy plays an important role in bounding the number of uniformly distributed bits that can be extracted from n samples. Hence, the Shannon entropy gives us a notion of how many samples are required to extract a certain degree of randomness, while the min-entropy gives us the worst-case randomness of a single sample. In either case, the higher the entropy, the better.

TABLE I
Simulated Circuit Parameters. $R_{N2,N3,P2}$ is the modeled total effective resistance of transistors $N2, N3, P2$.

Feature	Value	Feature	Value
NFET operation gate voltage	$1.5V$	R_{on}	1000Ω
PFET operation gate voltage	$0V$	R_{off}	2500Ω
$R_{N2,N3,P2}$, 2-bit TRNG	4450Ω	V_{init}	$0.8V$
$R_{N2,N3,P2}$, 4-bit TRNG	3440Ω	T_{enable}	$10ns$
$R_{N2,N3,P2}$, 6-bit TRNG	2640Ω	C	$10pF$
$R_{N2,N3,P2}$, 8-bit TRNG	1960Ω	Temp.	$300K$

B. Simulation Methodology

We evaluated our TRNG with Monte-Carlo simulations for the Enable step for different topologies, each with a different number of MTJ devices. The simulation numerically solves the differential equation system of the MTJs (stochastic LLG equations) and the capacitor. The transistors $N2, N3$, and $P2$ were modeled by a constant resistance. The equations were solved using a standard midpoint scheme [11] assuming no external magnetic field and the stochastic term was interpreted in the sense of Stratonovich.

Each iteration of the Monte-Carlo simulation produces the TRNG output binary word. For each measurement of entropy, 2000 iterations were conducted. The probability of each outcome was evaluated as its frequency of appearance. However, when the MTJs were identical, the probability was evaluated as the frequency of the corresponding Hamming weight divided by the number of outcomes with the same Hamming weight.

The STT-MTJ device is modeled as device C from [7]. The circuit parameters are listed in Table I. Different values for the modeled effective resistance of the transistors $N2, N3$, and $P2$ were simulated for each topology, and were chosen to maximize the entropy; results are shown in Table I. To find the size of the transistors and verify the accuracy of the constant resistance model, we performed circuit simulations (with resistors instead of MTJs) in Cadence Virtuoso using a 28nm GF process. Additionally, we measured the parasitic capacitance and leakage currents in our design. The simulation shows that the parasitic values are several orders of magnitude lower than the non-parasitic values, and hence they are ignored.

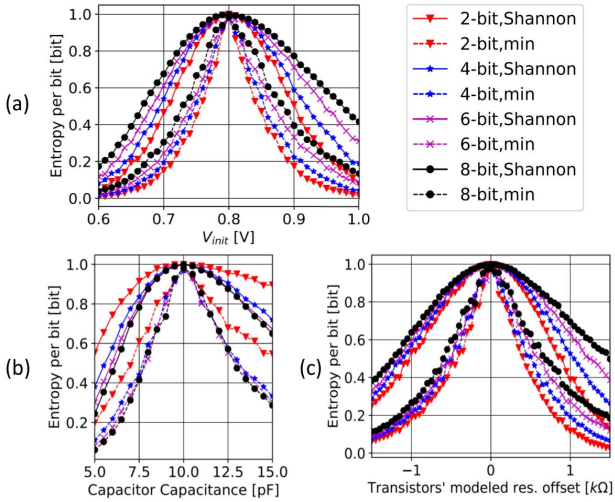


Fig. 2. The entropy of the TRNG for different (a) V_{init}, (b) C, and (c) offset in the modeled total effective resistance of the transistor $(N2, N3, P2)$.

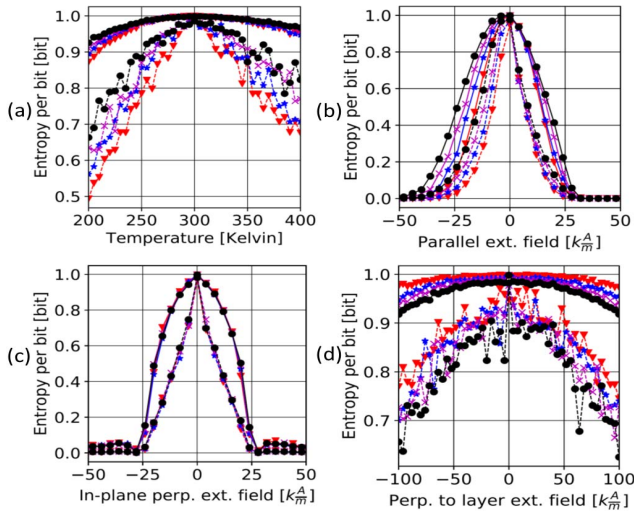


Fig. 3. (a) Effect of temperature. (b)-(d) Effect of a constant external magnetic field in fixed directions (b) parallel to the fixed layer magnetization, (c) in-plane and perpendicular to the fixed layer magnetization, and (d) perpendicular to the layer's plane. Legend as in Figure 2.

The TRNG simulation model does not include the correlation between consecutive runs of the TRNG; namely, our methodology assumes that the TRNG is an i.i.d. source. This is justified since the MTJs are always in the AP state prior to the Enable step. This results in a fresh start in every run, making the assumptions of an i.i.d. sequence reasonable. Nevertheless, consecutive runs will be correlated in a real-world TRNG. Some correlation will be caused by changes in the operation parameters but not by true causality between samples.

C. Entropy per Output

We evaluated the entropy of the TRNG for different design, environmental and process parameters.

1) Design Parameters: V_{init}, C, and the effective modeled resistance of $N2, N3$, and $P2$. Simulation results are shown in Figure 2. An important observation is that our design can, in the ideal case, reach nearly the maximum possible entropy (1-bit entropy per MTJ device).

It is evident that a small change in V_{init} can change the entropy. However, reasonable variations in the capacitance of the capacitor (less than $0.5pF$) have little effect on the entropy, since the designed value for the capacitance is relatively large.

2) Environmental Parameters: These parameters are external to the TRNG and can be altered by an adversary. The effect of temperature and the external magnetic field on the MTJ devices are considered here, and their influence on the entropy is shown in Figure 3. In our simulations, the temperature affects only the thermal fluctuations of the MTJs.

It is evident that a manipulation of the external magnetic field on the TRNG (by an attacker or unintentionally) can decrease the entropy substantially. Passive shielding is a way to mitigate the effect of an external field. Prior work [12], [13] on passive shielding demonstrated this for MTJ-based memories. Another approach is detection. This can be done using a dedicated magnetic sensor or with online tests.

3) Process Variation: Variations in both the MTJs and the transistors operating in the Enable step were considered. For the transistors, we modeled variations in their fixed resistance. For the MTJ, we modeled variations in the physical size of the devices: major and minor axis length (the MTJ shape is an ellipse cylinder [7]), the thickness of the free layer, and the thickness of the oxide layer (tunnel barrier layer). We generated 1000 different instances for each TRNG topology and their entropy was evaluated. The parameters were drawn independently from a Gaussian distribution with mean as the designed value and a standard deviation of 5%.

The physical dimensions of the MTJ affect its demagnetization factors [7] and resistance. The method presented in [14] was used to compute the new demagnetization factors. The MTJ resistance is proportional to the exponent of the oxide layer thickness and inversely proportional to its area [15]. The thickness of the oxide layer appears in the simulation only as part of the MTJ resistance. Since the oxide layer thickness is unavailable for the simulated device, the process variation for it was evaluated as an additional variation in the MTJ resistance by a Gaussian distribution with a standard deviation of 5%. The simulation results are listed in Table II. The results show that the entropy per bit increases with the number of MTJs, resulting in a twofold increase in the TRNG entropy.

D. Entropy Generating Rate

In many systems, a large number of entropy bits are required. In this case, the entropy generating rate (entropy bits per second) is the desired performance measure. Since many TRNG outputs are involved, the Shannon entropy is used here.

The Reset step duration is dominated by the capacitor charging time. If we model the pass-gate $P1 - N1$ (Figure 1) as a resistor of $1.5K\Omega$, the capacitor charging time from $0V$ to $0.79V$ is $66ns$. The duration of the Enable step is $10ns$ (Table I). In the Read step, the states of the MTJs are read using sense amplifiers. If we take the read latency of $2.8ns$ reported by [16], an output is produced every $78.8ns$.

For an 8-bit TRNG, 90% of the instances have an entropy generating rate between $79.2Mbps$ and $101.5Mbps$. This

TABLE II
ENTROPY RESULTS WITH PROCESS VARIATION SHOWING THE AVERAGE, STANDARD DEVIATION, MEDIAN, AND THE 10TH PERCENTILE. FOR THE 8-BIT TRNG WE SIMULATED 6000 ITERATIONS INSTEAD OF 2000.

	Shannon Entropy per Bit				Min-Entropy per Bit			
N	Avg.	sd	Med.	P_{10}	Avg.	sd	Med.	P_{10}
2	0.74	0.19	0.76	0.46	0.46	0.21	0.47	0.17
4	0.79	0.12	0.80	0.64	0.51	0.14	0.51	0.33
6	0.82	0.08	0.83	0.72	0.54	0.10	0.55	0.41
8	0.86	0.06	0.86	0.78	0.58	0.08	0.59	0.47

rate can be improved by terminating the Enable step earlier (since the switching probability is negligible before $10ns$) and by reducing the charging time (since the capacitor is not fully discharged immediately after an operation). For an 8-bit TRNG, the entropy generation rate can be improved to $99.7 - 127.8Mbps$ for 90% of the instances. Table III shows generation rates and comparison with other TRNGs.

E. Area and Energy

The STT-MTJ device area is $0.003\mu m^2$ [7]. To find the capacitor C area, we modeled it as a MOS capacitor with 28nm GF technology and obtained an area of $400\mu m^2$. We evaluated the sense amplifier area from [16] as the summed area of its transistors. All transistors were evaluated with a width of $1\mu m$ and minimum length ([16] does not specify transistor sizes). (This size upper bounds the area of the transistors shown in Figure 1.) The resulting area of an MTJ module is $0.78\mu m^2$. The sense amplifier in [16] uses an additional capacitor, but it is small since the read duration is $2.8ns$. Hence, each MTJ module area was evaluated as $1\mu m^2$. Table III lists the TRNG area for different N.

The TRNG consumes energy in the Reset and Read steps for capacitor charging, switching from P to AP of the MTJs (at the Reset step), and for the read operation. The Enable step only uses the energy stored in the capacitor. The energy required to charge the capacitor is the energy the capacitor holds, $3.2pJ$, plus another $3.2pJ$ consumed on the pass-gate before it (transistors $N1$ and $P1$ in Figure 1), for a pass-gate resistance of $1.5K\Omega$ and Reset step time of $66ns$. The MTJs have a write energy of $4.5pJ$ and a read energy of $0.7pJ$ [16]. Table III lists the energy for different N. As seen in Table III, STT-ANGIE has high entropy generation rate and low energy per entropy compared to CMOS TRNGs with a similar area.

V. CONCLUSIONS

In this paper, we presented STT-ANGIE, an asynchronous TRNG that uses STT-MTJ devices, utilizing the random switching time of the STT-MTJ devices. The TRNG was evaluated in simulations using the physical equations describing the STT-MTJs. The evaluation showed that by increasing the number of STT-MTJs in the design, the TRNG can have grater entropy per output and better resilience to process variation. Furthermore, the design achieves better throughput than that of current CMOS TRNGs, with lower energy per bit and similar die area. However, additional countermeasures are required to prevent attacks implemented by controlling the external magnetic field.

TABLE III
COMPARISON OF ENTROPY GENERATION RATE, AREA, AND ENERGY OF STT-ANGIE WITH PUBLISHED CMOS TRNGS. THE NUMBERS FOR STT-ANGIE ARE PRESENTED FOR 90% OF THE INSTANCES.

	Entropy Generation Rate [Mb/s]	Area [μm^2]	Energy [pJ/entropy-bits]
2-bit STT-ANGIE	16.2-35.1	402	8.4-18.3
4-bit STT-ANGIE	43.1-67.3	404	6.8-10.6
6-bit STT-ANGIE	70.6-98.0	406	6.3-8.7
8-bit STT-ANGIE	99.7-127.8	408	6-7.7
Yang *et al.* [17]	23.16	375	23
Srinivasan *et al.* [18]	2400	4004	2.9

ACKNOWLEDGMENTS

This research was partially supported by the Viterbi Fellowship at the Technion Computer Engineering Center, by Cisco grant no. CG679001, by the Technion Hiroshi Fujiwara Cyber Security Research Center, and by the Israel Cyber Bureau.

REFERENCES

[1] E. I. Vatajelu *et al.*, "STT-MTJ-Based TRNG With On-The-Fly Temperature/Current Variation Compensation," in *IOLTS 2016*.
[2] A. Fukushima *et al.*, "Spin Dice: A Scalable Truly Random Number Generator Based on Spintronics," *Appl. Phys. Express*, Vol. 7, No. 8, p. 083001, 2014.
[3] S. Oosawa *et al.*, "Design of an STT-MTJ Based True Random Number Generator Using Digitally Controlled Probability-Locked Loop," in *NEWCAS 2015*.
[4] S. Ghosh, "Spintronics and Security: Prospects, Vulnerabilities, Attack Models, and Preventions," *Proc. IEEE*, Vol. 104, No. 10, pp. 1864-1893, Oct 2016.
[5] S. P. Vadhan, "Pseudorandomness," *Found. Trends Theor. Comput. Sci.*, Vol. 7, No. 1-3, pp. 1-336, 2012.
[6] T. Devolder *et al.*, "Single-Shot Time-Resolved Measurements of Nanosecond-Scale Spin-Transfer Induced Switching: Stochastic Versus Deterministic Aspects," *Phys. Rev. Lett.*, Vol. 100, p. 057206, Feb 2008.
[7] A. F. Vincent *et al.*, "Analytical Macrospin Modeling of the Stochastic Switching Time of Spin-Transfer Torque Devices," *IEEE Trans. Electron Devices*, Vol. 62, No. 1, pp. 164-170, Jan 2015.
[8] T. L. Gilbert, "A Phenomenological Theory of Damping in Ferromagnetic Materials," *IEEE Trans. Magn.*, Vol. 40, No. 6, pp. 3443-3449, Nov 2004.
[9] García-Palacios *et al.*, "Langevin-Dynamics Study of the Dynamical Properties of Small Magnetic Particles," *Phys. Rev. B*, Vol. 58, pp. 14937-14958, Dec 1998.
[10] J. Slonczewski, "Current-Driven Excitation of Magnetic Multilayers," *J. Magn. Magn. Mater.*, Vol. 159, No. 1, pp. L1-L7, 1996.
[11] M. d'Aquino *et al.*, "Midpoint Numerical Technique for Stochastic Landau-Lifshitz-Gilbert Dynamics," *J. Appl. Phys.*, Vol. 99, No. 8, p. 08B905, 2006.
[12] K. Yamada, "Anisotropic Magnetic Shielding Effectiveness of Magnetic Shielded Package," *IEEE Trans. Magn.*, Vol. 53, No. 11, pp. 1-4, Nov 2017.
[13] W. Wang *et al.*, "Magnetic Shielding Design for Magneto-Electronic Devices Protection," *IEEE Trans. Magn.*, Vol. 44, No. 11, pp. 4175-4178, Nov 2018.
[14] D. Goode *et al.*, "The Demagnetizing Energies of a Uniformly Magnetized Cylinder With an Elliptic Cross-Section," *J. Magn. Magn. Mater.*, Vol. 267, No. 3, pp. 373-385, 2003.
[15] J. Li *et al.*, "Modeling of Failure Probability and Statistical Design of Spin-torque Transfer Magnetic Random Access Memory (STT MRAM) Array for Yield Enhancement," in *DAC 2008*.
[16] Q. Dong *et al.*, "A 1Mb 28nm STT-MRAM With 2.8ns Read Access Time at 1.2V VDD Using Single-Cap Offset-Cancelled Sense Amplifier and In-Situ Self-Write-Termination," in *ISSCC 2018*.
[17] K. Yang *et al.*, "16.3 A 23Mb/s 23pJ/b Fully Synthesized True-Random-Number Generator in 28nm and 65nm CMOS," in *ISSCC 2014*.
[18] S. Srinivasan *et al.*, "2.4GHz 7mW All-Digital PVT-Variation Tolerant True Random Number Generator in 45nm CMOS," in *Symposium on VLSI Circuits 2010*.