Binary and Ternary True Random Number Generators Based on Spin Orbit Torque

Huiming Chen[1,*], Shuai Zhang[1,*], Nuo Xu[2], Min Song[3], Xin Li[1],Ruofan Li[1], Yi Zeng[1], Jeongmin Hong[1], Long You[1§]
[1]School of Optical and Electronic Information, Huazhong University of Science and Technology, Wuhan 430074, China.
[2]Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, CA 94720, USA.
[3]Faculty of Physics and Electronic Science, Hubei University, Wuhan 430062, China.
[*]authors contributed equally to this work; [§]Email: lyou@hust.edu.cn

Abstract—In this work, we have experimentally demonstrated the binary- and ternary- True Random Number Generators (B-TRNG and T-TRNG) based on the stochastic switching characteristics of the nano-scale Ta/CoFeB/MgO heterostructures with perpendicular magnetization anisotropy. For the first time, the random code generation utilizes the spin orbit torque (SOT) induced by current flowing in the heavy metal underneath the CoFeB layer. The 3-XOR post-processed random binary codes have passed the NIST SP800-22 test. Furthermore, the T-TRNG in the same ferromagnetic heterostructure with dual magnetic domains are also demonstrated, which provides a higher security level than its B-TRNG counterpart.

INTRODUCTION

Hardware True Random Number Generator (TRNG) is an important security primitive which can generate random codes used for cryptographically secure information storage and encrypted data transmission of the modern communication systems [1]. Traditional CMOS based TRNGs rely on physical noise such as thermal noise, burst noise and oscillatory jitters, which require extensive post-processing to ensure a high level of randomness, resulting in a severe power, latency and area overhead [2]. While Spin-Transfer-Torque Magnetic Random-Access Memory (STT-MRAM) devices have inherent switching stochasticity due to thermal fluctuation fields, can potentially contribute to TRNG implementations [3-5]. With additional advantages of low operating voltages and high device density, STT-MRAM has attracted considerable research interests [6-8]. However, as shown in Fig. 1, write success rate (WSR) based STT-MRAM TRNGs require picosecond resolution of pulse width as well as an accurate write voltage control to reach the 50% randomness, making it non-trivial for practical applications [3]. On the other hand, write time (WT) based STT-MRAM TRNGs rely on several operation cycles to code one random bit [4,5], imposes a non-reducible power consumption and latency. Furthermore, the electrical stress-induced MgO/CoFeB interface degradation [8,9] and relatively high device-to-device mismatch in scaled STT-MRAMs [9] hinders this emerging technology towards a reliable TRNG solution. Using the Spin Orbit Torque (SOT) generated in a Ta/CoFeB/MgO heterostructure with perpendicular magnetization anisotropy (PMA) to switch the ferromagnetic layer has been proposed for low-power logic and memory devices because of their superior power efficiency, fast switching speed [10] and improved endurance due to the separation of read and write paths in this structure [11]. As shown in Fig. 2, when an in-plane current flows through the Ta layer along the *x*-direction, the spins will accumulate at the Ta/CoFeB interface due to the spin Hall effect (SHE). The switching is deterministic with the assistance of in-plane magnetic fields [12], exchange coupling [13] or breaking of geometrical symmetry [14], while under current-only operations on conventional SOT heterostructure, it results in a stochastic switching [15]. This stochastic behavior can be utilized as an ideal entropy generation source for a TRNG. In this work, for the first time, we proposed and experimentally demonstrated a TRNG based on SOT-induced stochastic switching in a PMA nano-ferromagnets (FM).

DEVICE CONCEPT AND FABRICATION

The principle of B-TRNG implemented by a FM layer with single domain structure is described in Fig. 3. First, a write current is applied to excite the FM to align its magnetization along the hard axis (in-plane directions). After the write current is removed, the magnetization orientation is driven to the easy axis (out-of-plane direction). Depending on the thermal fluctuations, the magnetization either goes 'upward' or 'downward', creating the random code. The switching speed of the PMA nanomagnet with single domain can be very fast, based on experimental results [16] and from our macro-spin simulations. As shown in Fig.4(a), one random switching operation requires no more than 3 ns. Furthermore, Fig. 4(b) and (c) indicate that the switching probability (P_{sw}) is insensitive to both current and temperature variation in a board range, proving its robustness under different operating conditions. As for the T-TRNG, the ternary state may originate from the domain wall (DW) propagation in dual-domain nano-FMs. The applied write current results in three random final states: (1) there are neither nucleation nor DW motion induced [Fig.5(d)]; (2) a DW is created but pinned at the middle of the FM layer during its motion [Fig.5(e)]; and (3) a DW is created and propagates to the end of the structure, causing a full magnetization reversal [Fig.5(f)].

A FM layer stack comprising Ta (10 nm)/CoFeB (1.2 nm)/MgO (1.6 nm)/Ta (5 nm) was first deposited on thermally oxidized Si substrate. As shown in Fig. 6, the DW propagation has been observed in the Ta/CoFeB/MgO thin film by magneto-optical *Kerr* (MOKE) microscopy experiments. The SOT induced effective field are shown in Fig. 7. Therefore, it is considered that the ternary state results from the DW propagation in a relatively-large area, a dual-domains FM device. The Ta/CoFeB/MgO thin film was further processed into the Hall bar structure by electron beam lithography (EBL)

and argon-ion milling (AIM). The Hall bar contains the entire thin film stack and the region outside it was etched till the insulating SiO_2 substrate. A 10 nm thick hard mask (Ti) with sizes of 200×200 nm^2 and 500×500 nm^2 were grown at the center of the Hall bars by EBL and deposited by EB evaporation. AIM was then used to etch the stack outside the dot's region down to the bottom Ta layer. The smaller FM dot forms a single domain (for B-TRNG) while the lager one forms dual domains (for T-TRNG). All the fabrication was conducted at low temperature (from RT to less than 150°C). The optical and scanning electron microscope (SEM) images of B-TRNG and T-TRNG devices are shown in Fig. 8.

RESULTS AND DISCUSSION

A. Properties of the Ta/CoFeB/MgO Heterostructure

Fig. 9(a) shows the normalized R_{AHE}-H loops with different currents injected into the 200×200 nm^2 device. Clearly, the magnetic coercive field (H_c) decreases with the increasing current. The relationship between H_c and applied current is shown in Fig.9(b), indicating that current induced effective field (estimated as 2.5 Oe/(10^5A·cm^{-2})) favors the switching of Ta/CoFeB/MgO heterostructure. The SOT induced deterministic switching under external magnetic field is further shown in Fig. 9(c). On the other hand, the normalized R_{AHE}-H and R_{AHE}-I loops of the 500×500 nm^2 device are shown in Fig.10. The "rectangular" shape R_{AHE}-H loops suggest that both smaller- and larger-area devices have the dominant PMA with the easy axis along the out-of-plane (z) direction.

B. Performance of the Binary and Terbary TRNGs

The stochastic switching behavior of the B-TRNG device is shown in Fig. 11. The probability of upward and downward switching differs by 2.0% from measurement of 100 cycles. Fig. 12 shows the circuit schematics of the B-TRNG with detailed working principles elaborated in Fig. 13. A current pulse I_a [Fig. 13(a)] with fixed width is applied across the Hall bar along x axis, while the AHE voltage V_b [Fig. 13(b)] is measured along y axis. The write current has an amplitude of 0.5 mA (1.0×10^7 A/cm^2) and duration of 0.5s, and afterward a read current with an amplitude of 50 μA and duration of 1s is applied. V_b is determined by the magnetization orientation. When magnetization aligns upward, V_b is higher than the reference voltage (V_{ref}, the average of highest and lowest V_b), the output voltage (V_c) of the comparator goes to logic high level ('1'). In contrast, when magnetization aligns downward, V_b is lower than V_{ref} and V_c falls to logic low level ('0'). A sampling clock V_{clock} with a fixed duty cycle (Fig. 13(d)) and V_c are sent to an AND gate. The V_c in the period of the low I_a is sampled as the output of the B-TRNG. In this way, the output (a '0-1' code sequence) is distributed randomly due to the stochastic switching of the magnetization. A sequence of ~20k random bits generated by the B-TRNG with the raw data shown in Fig. 14(a) and the statistical results in Fig. 14(b), which indicates that the cases of upward and downward switching are different by 4.4%. After 3 times XOR post-processing (Fig. 15), the output codes can pass the NIST SP800-22 test [17] as shown in TAB I.

The stochastic switching behavior of the T-TRNG device is studied in Fig. 16. The P_{sw} of the three states varies with the current pulse amplitude. The operation window for T-TRNG lies between 1.7 – 1.9mA. Therefore, 1.8 mA is chosen as the operation current level. Fig. 17 shows the circuit schematics of the T-TRNG with detailed illustrations in Fig. 18. Similar to B-TRNG, the write current pulse I_a is 1.8 mA/1s (Fig. 18(a)), while the read current is 50 μA/1s. Two comparators are used since the AHE voltage V'_b (Fig. 18(b)) is ternarily distributed. The resulted two reference voltages $V_{ref,h}$ and $V_{ref,l}$ are set as $3/4V'_{b,max}+1/4V'_{b,min}$ and $1/4V'_{b,max}+3/4V'_{b,min}$, as show in Fig. 17(c) and (d), respectively. The outputs of each comparators are sent to its associative AND gates. The sampling clock V_{clock} is used as the other inputs of the two AND gates, as shown in Fig.17. Two individual binary codes will be output from this setup as shown in (Fig. 18(e), and (f)). Then, the two sequences are sent to a decoder to generate ternary random sequence. A statistical result of 390k bits ternary sequence generated by T-TRNG is shown in Fig. 19, in which the maximum switching probability differences are ~1.88% from 390k measurements. The T-TRNG can provide a higher security than the B-TRNG with same sequence size. One can calculate the largest possible combination based on a 100-bit ternary sequence to be 5.15×10^{47}, which is 17 orders of magnitude more than that of a 100-bit binary sequence (with total combination numbers of 1.27×10^{30}).

C. Future Directions of SOT-TRNGs

TAB. II summarizes the work SOT-based TRNG's features, which are further compared against and compares to previously reported TRNGs [2-5]. Additionally, the current density for SOT devices can be reduced significantly through applying heavy metal with larger spin Hall angle (θ_{SH}). According to $\theta_{SH} = J_S/J_e$, where J_e is the charge current density and $[\hbar/(2e)]J_S$ is the spin current density arising from the SHE [12], required current decreases linearly with θ_{SH}. For example, by using β-W ($\theta_{SH,\beta\text{-}W} = 0.33 \pm 0.06$ [18], which is dozens of times that of compared to the Ta ($\theta_{SH,Ta} \sim 0.007$) [15]), operating current (power) can be lowered remarkably as demonstrated in this work. Besides, the low temperature fabrication of demonstrated TRNGs makes them promising for monolithic-3D integration into the standard CMOS back-end-of-line (BEOL) process flow. It is also feasible to integrate high-density SOT-TRNG arrays by accommodating the BEOL-embedded memory hierarchy, in which the logic peripheries (e.g. comparators and XOR gates, etc.) can be shared by a column of the TRNG bit array, to reduce the chip area.

CONCLUSIONS

The stochastic switching properties of the PMA MgO/CoFeB/Ta heterostructure have been demonstrated using current induced SOT. By tuning the device's size, either single or double domains can be formed within the CoFeB layer for Binary or Ternary TRNG applications, respectively. The random codes generated by B-TRNG with 3-stage XOR post-processing have passed the NIST SP800-22 test. Meanwhile, the code sequences produced by T-TRNG show high quality of randomness, guaranteeing a better security level. In comparison with other STT-MRAM based TRNG implementations, this work proposes a potential solution to achieve high device reliability and integration density, thanks to the SOT effect.

Acknowledgment: Authors acknowledges financial support from the National Natural Science Foundation of China (NSFC Grant No. 61674062 and No. 61821003), the Fundamental Research Funds for the Central Universities (HUST: 2018KFYXKJC019) and the Thousand Young Talents Program of China.

REFERENCES

[1] H. Jiang *et al*., *Nat. Comm.*, 8, 882, 2017. **[2]** K. Yang *et al*., *IEEE ISSCC Tech. Dig*., pp. 280-282, 2014. **[3]** W. H Choi et al., *IEEE IEDM* pp. 12.5.1-12.5.4, 2014. **[4]** R. Carboni *et al*., *IEEE EDL*, pp.951-954, 2018. **[5]** K. Yang *et al*., *IEEE VLSI Symp. Circ*., pp.171-172, 2018. **[6]** M. Manfrini *et al., AIP Advances* 8.5, 055921, 2018. [7] DE. Nikonov *et al., IEEE EDL* 32.8, pp.1128-1130, 2011. **[8]** R. Carboni *et al*., IEEE IEDM Tech. Dig., pp.572-575, 2016. **[9]** N. Xu *et al*., *IEEE VLSI Symp. Tech*., pp.187-188, 2018. **[10]** G.Prenat et al., *IEEE Trans. Multi-Scale Computing Systems*, pp 49-60 ,2016. **[11]** G. Prenat et al., *Spintronics-based Computing*. Springer, Cham, pp.145-157, 2015. **[12]** L. Liu *et al*., *Science*, pp. 555-558, 2012. **[13]** Y.-C. Lau *et al*., *Nat. Nanotechnol*., 11, pp. 758-762, 2016. **[14]** L. You *et al*., *PNAS*. pp. 10310-10315, 2015. **[15]** G. Yu et al., *Nat. Nanotechnol.,* 9, pp. 548–554 ,2014. **[16]** M. Cubukcu et al., *IEEE Trans. Magnetics* 54.4 pp. 1-4, 2018. **[17]** A. Rukhin et al., NIST SP 800-22 test suites, 2010. **[18]** C. F. Pai et al., *Appl. Phys. Lett.*,101, 122404, 2012.

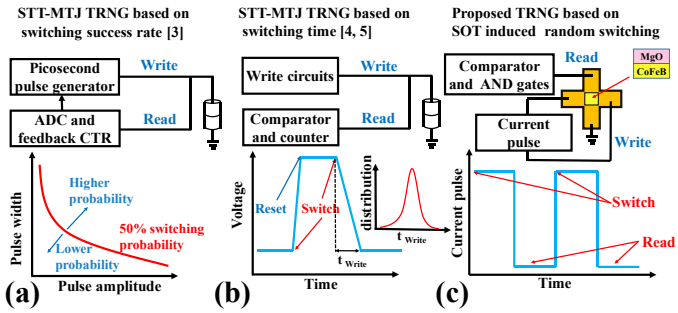

Fig. 1: Illustrations of random coding principles for STT-MRAM based (a) WSR-TRNG [3] and (b) WT-TRNG [4, 5]; and (c) proposed SOT-based TRNG.

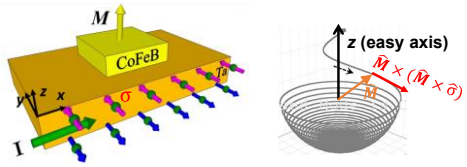

Fig. 2: The schematic of the SOT induced switching of a PMA ferromagnet (FM). Switching current is applied in the underneath heavy metal layer.

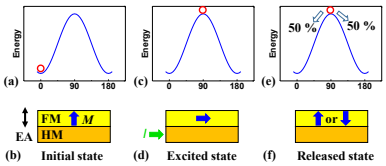

Fig. 3: Schematic of the principle of B-TRNG, with (a, b) as the initial state. In (c, d), a write current is applied to excite the FM to align its magnetization along the hard axis. When it is turned off (e, f), the magnetization is driven back to the easy axis by the PMA.

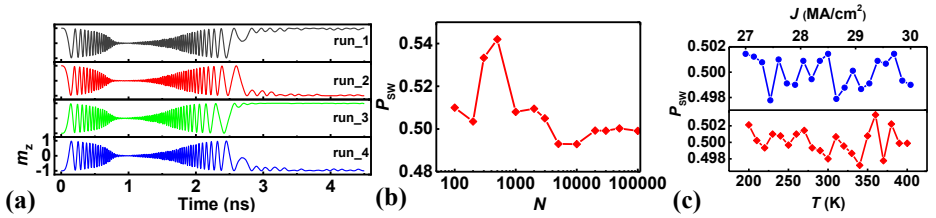

Fig. 4: Macro-spin simulation of random switching of a single FM domain, showing (a) four stochastic switching cases induced by the SOT; (b) the accumulative switching probability (P_{sw}) *vs*. number of switching cycles; and (c) P_{sw} as a function of temperature (T) and applied current density (J), showing only small fluctuations.

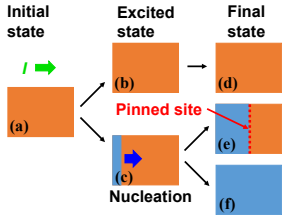

Fig. 5: Schematic of the principle of T-TRNG, with all possible stable states due to multi-domain effects and current induced DW propagation.

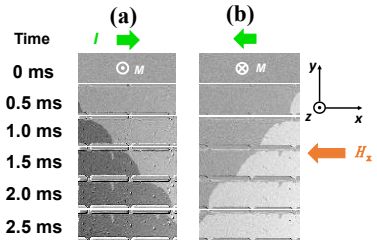

Fig.6: MOKE images of DW motion induced by SOT in a continuous Ta/CoFeB/MgO film.

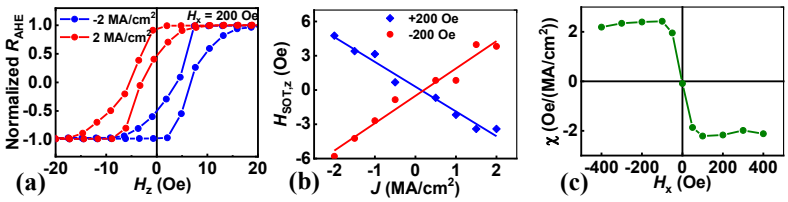

Fig. 7: Characterizations of the Ta/CoFeB/MgO thin film, showing (a) measured AHE loop shift induced by SOT effective filed, (b) the relationship between SOT induced effective field and current density, and (c) DMI effective field efficiency as a function of external field.

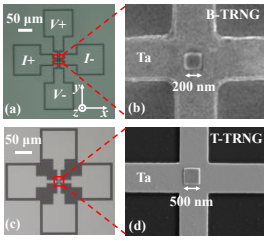

Fig. 8: Optical (a, c) and SEM (b, d) images of fabricated B-TRNG (a, b) and T-TRNG (c, d) devices.

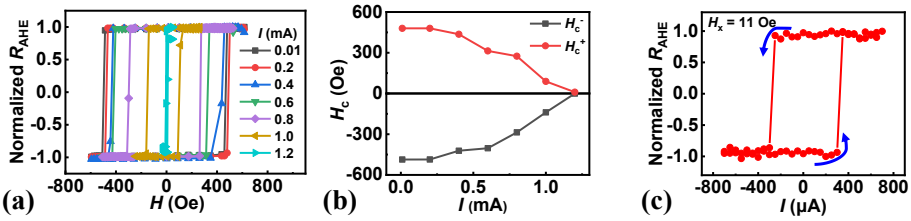

Fig. 9: Characterizations of the B-TRNG device, with (a) AHE loops under different currents, (b) H_c varies with currents, (c) SOT induced deterministic switching with the help of an external field.

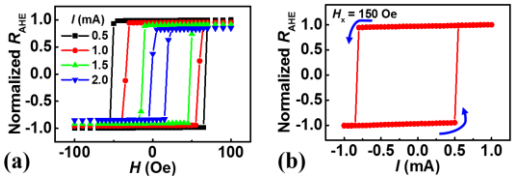

Fig. 10: Characterizations of the T-TRNG device, with (a) AHE loops under different switching currents and (b) SOT induced deterministic switching of T-TRNG with the help of an external field.

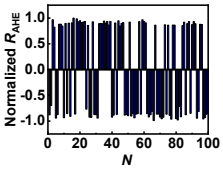

Fig. 11: SOT induced stochastic switching without external field, for 100 cycles.

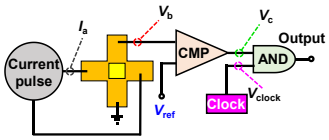

Fig. 12: The schematic circuits of the B-TRNG.

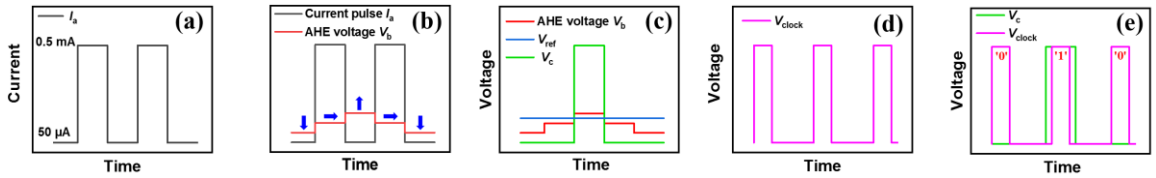

Fig. 13: Schematic waveforms at each stage of the B-TRNG circuit. (a) Input current pulse. (b) AHE voltage V_b obtained utilizing the read current of (a). Blue arrows represent magnetization. (c) V_b is transformed to logic voltage V_c by a comparator. (d) Sampling clock signal. (e) The random code bits are generated from the output of the AND gate.

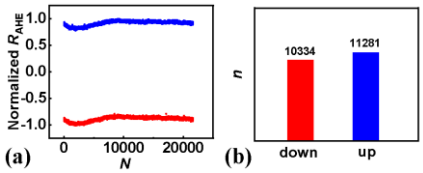

Fig. 14: The SOT induced stochastic switching of the B-TRNG without external field, with (a) the distribution of ~20k random switching results and (b) the switching probability.

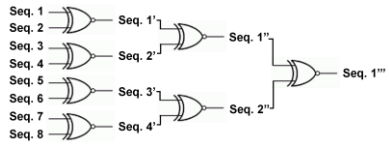

Fig. 15: The schematic of the post-processing XOR operation for the B-TRNG.

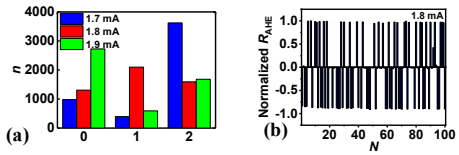

Fig. 16: The SOT induced stochastic switching of T-TRNG without external field, with (a) switching probability dependence on current pulse amplitude and (b) 100 random switching results of the T-TRNG.

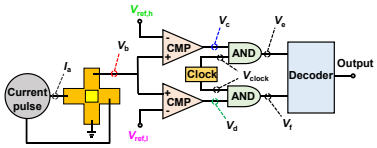

Fig. 17: The schematic circuits of the T-TRNG.

	P-value	Pass rate	Success/failure
Frequency	0.709991	2/2	Success
Block Frequency	0.806341	2/2	Success
Cumulative Sums	0.876773	2/2	Success
Runs	0.733546	2/2	Success
Longest Run	0.443576	2/2	Success
Rank	0.333851	2/2	Success
FFT	0.036257	2/2	Success
Non Overlapping Template	-	290/296	Success
Overlapping Template	0.830234	2/2	Success
Serial	0.659356	4/4	Success
Linear Complexity	0.695952	2/2	Success

TAB I: The NIST SP800-22 test results after post-processing using XOR gates shown in Fig.14. (A 7k bits sequence was divided into two segments, P-value > 0.01, and proportion > 290/296)

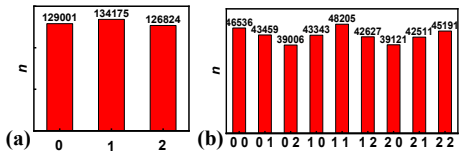

Fig. 19: The distribution of 390k random switching results from the T-TRNG. (a) Distribution of final states, with "0", "1" and "2" represent the low, medium and high resistance state, separately. (b) Distribution of switching events. "X Y" represents that 'X' switches to 'Y' state.

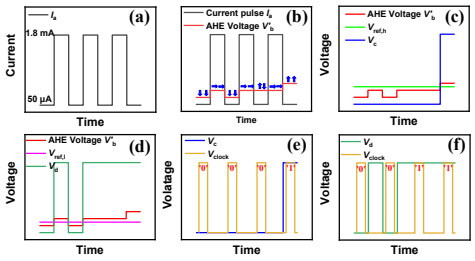

Fig. 18: Schematic waveforms at each stage of the T-TRNG circuit. Input current pulse. (b) AHE voltage V'_b obtained utilizing the read current of (a). Blue arrows represent magnetization. (c), (d) show the ternary V'_b is transformed to two logic voltage V_c and V_d by two comparators. (e), (f) The random bits are generated from the output of the AND gates.

	This work		ISSCC'14 [2]	IEDM'14 [3]	VLSI' 18 [4]	EDL'18 [5]
	B-TRNG	T-TRNG				
Entropy source	SOT Switching		Thermal Nosie	STT Switching	STT Switching	STT Switching
Area(μm²)	0.04 (Magnet only)	0.25 (Magnet only)	375	0.008 (MTJ Only)	180	N/A
NIST 800-22 TEST PASSED	11	N/A (Not Suitable)	All	10	All	10
Post proceeding	Yes (3 XOR Operation)	No	Yes (extensive)	Yes (Von Neumann Correction)	No	No

TAB II: Summary of the features of SOT-based TRNG in this work and STT-MRAM based TRNGs reported in [2-5].