SCIENCE CHINA
Information Sciences

• LETTER •

February 2026, Vol. 69, Iss. 2, 129403:1–129403:2
https://doi.org/10.1007/s11432-025-4595-5

High-performance true random number generator based on SOT-MTJ spin relaxation

Jialiang YIN[1,2†], Xiuye ZHANG[1†], Boyan ZHANG[1], Bolin ZHANG[1], Wenlong CAI[1], Ao DU[1], Binchao TANG[2], Haowei ZHANG[2], Shijian BAO[2], Chunyi LI[1], Daoqian ZHU[1], Kewen SHI[1], Hongxi LIU[3], Lang ZENG[1], He ZHANG[1*], Kaihua CAO[1*] & Weisheng ZHAO[1*]

[1]*Fert Beijing Institute, School of Integrated Circuit Science and Engineering, Beihang University, Beijing 100191, China*
[2]*China International Engineering Consulting Corporation, Beijing 100048, China*
[3]*Truth Memory Corporation, Beijing 100088, China*

Received 30 April 2025/Revised 1 July 2025/Accepted 12 September 2025/Published online 4 January 2026

Citation Yin J L, Zhang X Y, Zhang B Y, et al. High-performance true random number generator based on SOT-MTJ spin relaxation. Sci China Inf Sci, 2026, 69(2): 129403, https://doi.org/10.1007/s11432-025-4595-5

With the rise of artificial intelligence and the Internet of Things, security hardware—such as true random number generators (TRNGs)—has become essential for emerging computing and information security [1, 2]. However, the application prospects of conventional TRNG based on CMOS technology are limited due to challenges in the aspects of complex design structures, additional calibration requirements, and high power consumption. Recently, non-volatile memories have gained significant attention in the field of random number generation owing to their unique characteristics, including inherent entropy sources, low power consumption and high throughput. Among them, the spin-orbit torque magnetic tunnel junction (SOT-MTJ), a fundamental component of third-generation magnetic random access memory (MRAM), has emerged as a promising candidate for TRNGs due to its small footprint, fast writing speed, and high endurance [3].

High-barrier SOT-MTJs have demonstrated potential for random number generation by harnessing thermal field fluctuations during write operations [4]. However, the precise control required for the write current pulse width and amplitude has led to reliability issues in random number generation. To address this, a proposed scheme utilizes in-plane SOT current to switch perpendicular magnetization, naturally achieving 50% randomness between spin-up and spin-down states after current withdrawal [5]. Yet, this approach demands a larger SOT current, resulting in increased power consumption. An alternative solution involves low-barrier SOT-MTJs, designed as TRNGs that modulate probability outputs through energy-efficient circuits [6]. Nevertheless, process variations limit their scalability at the array level. Thus, designing a reliable, low-power, and scalable SOT-MTJ-based TRNG remains a significant challenge. Here, we propose a TRNG based on high-barrier in-plane SOT-MTJ that leverages the spin relaxation process as an entropy source to overcome these challenges.

Results. The schematic of the proposed TRNG, which utilizes spin relaxation as an entropy source, is shown in Figure 1(a). The device stack structure is specifically designed so that the reference layer (RL) provides an additional stray field for the TRNG (see Appendix A for device morphology characterization). Figure 1(b) presents the hysteresis loop of the SOT-MTJ, where a −2 mT stray field from the RL stabilizes the MTJ in an antiparallel state as the initial stable state. When an SOT current is applied across the SOT channel, the magnetization in the free layer (FL) rapidly transitions from this stable state to an unstable state. After the SOT current is withdrawn, the magnetization of the FL undergoes precession and spontaneously relaxes back to the stable state under the influence of random thermal fluctuations and the stray field (see Appendix A for the dynamic process of the SOT-MTJ). The relaxation time during this process is inherently random and unpredictable, making it a suitable entropy source for TRNG implementation.

A test setup has been proposed to verify the intrinsic physical properties of this entropy source (see Appendix B). Figure 1(c) demonstrates that, under the same stray field and identical SOT write current conditions, the device's relaxation time follows a Gaussian distribution, confirming that the relaxation time serves as a reliable entropy source. To account for the mutual influence of stray fields between devices in an array, statistical analysis of the relaxation time histograms under different magnetic fields has been conducted. The results indicate that, although the average relaxation time shifts τ_{relax}, the relaxation times under varying magnetic fields still follow Gaussian distributions. This observation confirms that the proposed entropy source exhibits robustness against magnetic field disturbances. Figure 1(d) illustrates that the τ_{relax} remains largely unchanged despite variations in the amplitude and pulse width of the SOT current. In other words, the proposed SOT-based TRNG exhibits robust, inherent resistance to electrical noise and thermal perturbations, eliminating the need for precise write voltage control and thereby enhancing device reliability. Additionally, the proposed SOT-based TRNG exhibits excellent endurance of $> 2 \times 10^{11}$ (see Appendix A).

In order to convert the analog time signal into binary digital

* Corresponding author (email: zhanghe@buaa.edu.cn, kaihua.cao@buaa.edu.cn, wszhao@buaa.edu.cn)
† These authors contributed equally to this work.

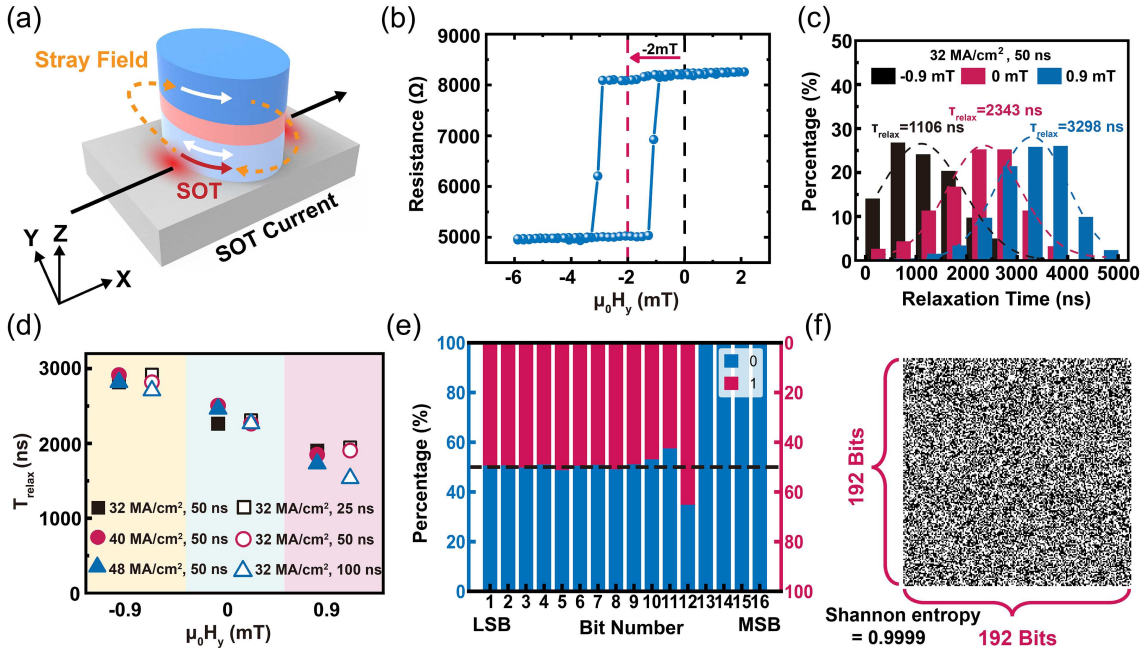

Figure 1 (Color online) (a) Schematic of the SOT-induced spin relaxation TRNG. (b) Hysteresis curve of MTJ resistance versus in-plane external magnetic field. (c) Histogram of the relaxation time under magnetic field modulation. (d) Mean relaxation time as a function of the amplitude and pulse width of SOT current in different magnetic fields. (e) Percentage of occurrence of '0' and '1' for each bit of the count output. (f) Grayscale pattern of the 36 kbits generated from a single TRNG. Black squares correspond to '0', and white squares correspond to '1'.

signal, a post-process peripheral circuit with sense amplifier (SA) and T flip-flops has been designed (see Appendix C). Figure 1(e) displays the percentage of occurrence of '0' and '1' for each bit after converting the relaxation time to the 16-bit random number stream. The first 10 least significant bits (LSBs) exhibit nearly equal probabilities, indicating that these LSBs can be directly used as random bits without any additional calibration. The Shannon entropy of each bit in the first 10 LSBs is close to 1 (see Appendix C). The proposed TRNG also exhibits good scalability, as demonstrated by the fabrication of devices with varying sizes (see Appendix D). Figure 1(f) shows the grayscale pattern of 36 kbits of random numbers generated from the same single device shown in Figure 1(b), under various external magnetic field and write pulse conditions. The corresponding Shannon entropy is 0.9999, demonstrating the high quality of the output. Furthermore, the excellent quality of the generated random numbers is validated using the NIST SP800-22 and NIST SP800-90B test suites. The 36864-bit random number sequences successfully pass both NIST tests without any post-processing (see Appendix C). Meanwhile, the autocorrelation function test is performed on the same random number sequence (see Appendix C). The throughput of a single device serves as a key metric for evaluating TRNG performance. For the proposed SOT-based TRNG, a speed of 4.3 Mbit/s is achieved by applying a 1 GHz clock signal. In addition to output speed and scalability, power consumption is also a critical performance metric for TRNGs. Based on simulations using a 40 nm process library in Cadence, the energy consumption of the proposed TRNG is estimated to be 24.6 pJ/bit (see Appendix E).

Conclusion. In this work, we propose a TRNG based on high-barrier in-plane SOT-MTJs, utilizing spin relaxation as the entropy source. The high-performance of the proposed TRNG is attributable to its excellent scalability, strong randomness, and high reliability. Additionally, it achieves good endurance exceeding 2×10^{11} cycles, high throughput of 4.3 Mbit/s, and ultra-low power consumption of 24.6 pJ/bit, making it well-suited for hardware security and large-scale integrated computing applications.

Acknowledgements This work was supported by National Key Research and Development Program of China (Grant No. 2022YFB4400200), National Natural Science Foundation of China (Grant Nos. T2394474, T2394470, 62271026, 623B2015, 62401026, 62404013), National Postdoctoral Program for Innovative Talents (Grant No. BX20240455), Beijing Natural Science Foundation (Grant No. 4232069), Beijing Outstanding Young Scientist Program, and Tencent Foundation through the XPLORER PRIZE.

Supporting information Appendixes A–E. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Cai W, Huang Y, Zhang X, et al. Spintronics intelligent devices. Sci China-Phys Mech Astron, 2023, 66: 117503
2 Zhang X, Jiang C, Yin J, et al. Experimental realization of physical unclonable function chip utilizing spintronic memories. Engineering, 2025, 49: 141–148
3 Guo Z, Yin J, Bai Y, et al. Spintronics for energy-efficient computing: an overview and outlook. Proc IEEE, 2021, 109: 1398–1417
4 Ng H J, Yang S, Yao Z, et al. Provably secure randomness generation from switching probability of magnetic tunnel junctions. Phys Rev Appl, 2023, 19: 034077
5 Chen H, Zhang S, Xu N, et al. Binary and ternary true random number generators based on spin orbit torque. In: Proceedings of IEEE International Electron Devices Meeting (IEDM), 2018
6 Yin J, Liu Y, Zhang B, et al. Scalable ising computer based on ultra-fast field-free spin orbit torque stochastic device with extreme 1-bit quantization. In: Proceedings of IEEE International Electron Devices Meeting (IEDM), 2022