NIST SP 800-90B Compliant Perpendicular Magnetic Tunnel Junction Based True Random Number Generator

Qi Jia[1], Shannon Egan[2], Yang Lv[1] and Jian-Ping Wang[1*]

[1]Department of Electrical and Computer Engineering, University of Minnesota, Minneapolis, MN 55455, USA,
[2]Deep Science Ventures, London, UK

True random number generators (TRNGs) are essential for applications such as hardware security and cryptographic protocols. Stabilized spin-transfer torque-perpendicular magnetic tunnel junctions (STT-pMTJs) have emerged as a promising candidate for TRNGs due to their rapid switching speed and low energy consumption. The switching speed could be controlled by the voltage amplitude, enabling high quality bit generation with adjustable frequency. In previous studies, the quality of the generated bits is evaluated by NIST 800-22 standards, which are now considered outdated and insufficient for modern cryptographic requirements. In this work, we demonstrate a pMTJ-based TRNG with a low resistance-area (RA) product of 3.5 Ω·μm² and a tunnel magnetoresistance (TMR) ratio of 105%. The magnetization switching occurs in 2.70 ns with a probability of 50% at a current density of 3.38×10^7 A/cm². The generated bits achieve NIST SP 800-90B compliance with only a single XOR whitening step.

***Index Terms*—Spintronics, True random number generators, Magnetic tunnel junction**

I. Introduction

True Random Number Generators (TRNGs) are crucial for hardware security and cryptographic protocols. Conventional CMOS-based TRNGs face significant challenges due to poor power efficiency, hindering their scalability and reliability [1]. Spintronic devices, particularly magnetic tunnel junctions (MTJs), offer a promising alternative due to their low power consumption and rapid switching capabilities [2]-[11]. Recent studies have demonstrated that STT-pMTJ-based TRNGs can achieve randomness verified by the NIST 800-22 test suite [9]-[11]. However, this test suite is now considered outdated and insufficient for modern cryptographic requirements [12]. In contrast, NIST SP 800-90B defines stricter criteria for entropy sources [13], making it a critical standard for secure hardware applications.

In this work, we present a pMTJ-based TRNG that achieves NIST SP 800-90B compliance with only a single XOR whitening step. Voltage pulses induce probabilistic switching in the pMTJ, and the resulting bitstream is processed with XOR to enhance entropy. The processed output successfully passes all NIST SP 800-90B statistical tests, marking it as a promising candidate for next-generation secure random number generation.

II. TRNGs by STT-MTJ

The perpendicular MTJs used in this work are based on pMTJ of the core structure of CoFeB / MgO / CoFeB stack. The detailed structure is Ta(3) / CuN(40) / Ta(3) / CuN(40) / Ta(3) / Ru(10) / Ta(5) / CoFeB(1) / MgO / CoFeB(1) / $[Co(0.3)/Pd(1)]_{10}$ / Ta(5) / Cu(10) / Ru(5) / Ta(3), with all thickness in nanometers. Pillar-shaped devices with a diameter of 80 nm were fabricated using e-beam lithography and ion milling. The resulting MTJs exhibit a tunneling magnetoresistance (TMR) ratio of 105% and a resistance-area (RA) product of 3.5 Ω·μm². STT was employed to achieve deterministic switching between the parallel (P) and antiparallel (AP) states of the MTJ.

Two pulse generators were used to apply voltage pulses across the pMTJ. One generator produced a high-amplitude, long-duration pulse to reliably reset the MTJ to its initial state. The second pulse generator was then triggered to deliver a perturbation pulse with opposite polarity to attempt switching. The resistance state of the MTJ was measured after each perturbation pulse using a longer read-out voltage pulse to determine whether switching occurred. The overall cycle time is 100 μs (10 kbps).

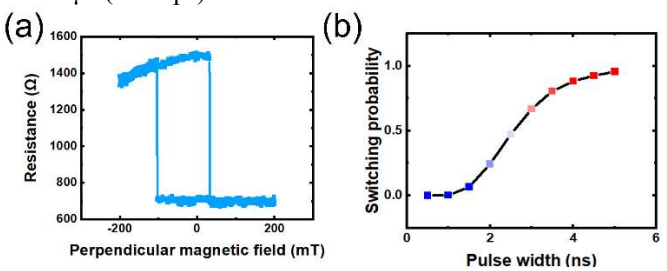

Fig. 1. (a) Resistance vs. perpendicular magnetic field, minor loop of the pMTJ. (b) Switching probability vs. perturbation pulse width of the pMTJ under fixed voltage of 1.19V. Test is at room temperature.

In the selected MTJ, whose R-H loop is shown in Fig. 1 (a), an out-of-plane magnetic field of -90 mT is applied to symmetrize the switching voltages for AP-to-P and P-to-AP transitions. In each trial, the MTJ was first reset to AP state using a -0.35 V, 500 ns pulse. The switching probability as a function of pulse width under a fixed pulse amplitude of 1.19 V is shown in Fig. 1(b). Each data point was obtained from 10,000 repeated trials. As the switching pulse width increases, the switching probability rises and approaches one, consistent with the nature of STT-induced switching. A 50% switching probability was achieved at a pulse width of 2.70 ns. To evaluate the randomness quality, we repeated the experiment under this condition and collected 10 million bits for statistical testing.

III. NIST Entropy Source Validation Testing

NIST SP 800-90B describes the validation process for entropy sources used in cryptographic random bit generation and is one of the key publications underpinning NIST's

Cryptographic Module Validation Program (CMVP) [13]. Under the SP 800-90B guidelines, random samples produced by a noise source may be evaluated according to the IID (independent and identically-distributed), or non-IID track. For the pMTJ-based TRNG, the binary outcome of each switching attempt (1 for a successful switch, 0 otherwise) is a Bernoulli random variable with switching probability p. Whether the IID assumption holds is primarily contingent on the stability of p across attempts (Fig. 2). If each switching attempt is an IID Bernoulli process, the number of successful switching events in n attempts should follow the binomial distribution with success probability p, i.e. X ~ B(n,p), where X is the observed number of AP-to-P switching events. XOR-whitened bitstreams using 2, 4, and 8 bits (abbreviated henceforth as XORk, where k is the number of bits) show excellent agreement with the statistics of a binomial distribution (Fig. 3), including the variance scaling as np(1-p) with the number of trials (Fig. 4), but raw bistreams do not. This simple analysis suggests that the IID assumption may be justified only for the XOR-whitened bitstreams.

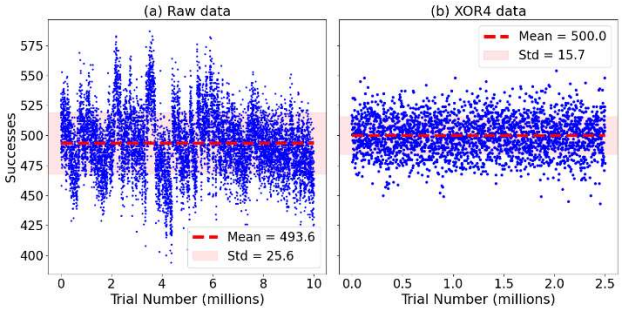

Fig. 2. (a) Number of successful switching attempts over 1000 trials for sequential samples of the raw bitstream. Visible clustering indicates that p is not constant for each set of switching attempts. (b) Number of 1's over 1000 values of the XOR4 bitstream.

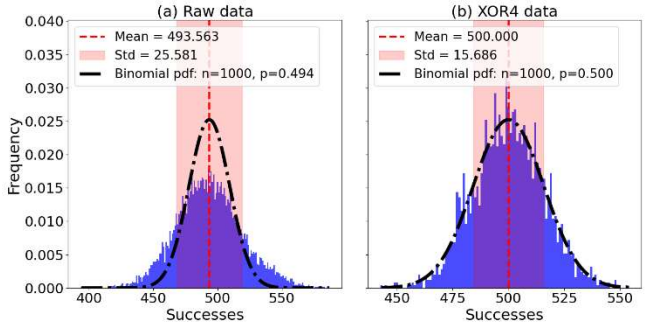

Fig. 3. Histogram of number of successful switching attempts over 1000 trials for sequential samples of the raw bitstream (a) and 4-bit XOR-whitened bitstream (b). In XOR4 data, the expected value and standard deviation of the sample mean show excellent agreement with a binomial distribution of $p = 0.5$ and $\sigma^2 = p(1-p)n = (15.811)^2$.

We ran all bitstreams through SP 800-90B IID track testing: the raw bitstream passes only 7/22 IID tests, while XOR2, XOR4, and XOR8 bitstreams pass all 22/22. This result forces us to reject the IID assumption in the raw bitstream but supports the IID assumption for XOR-whitened bitstreams. The final entropy estimated for each bitstream, each with different degrees of XOR whitening, is given in Table I.

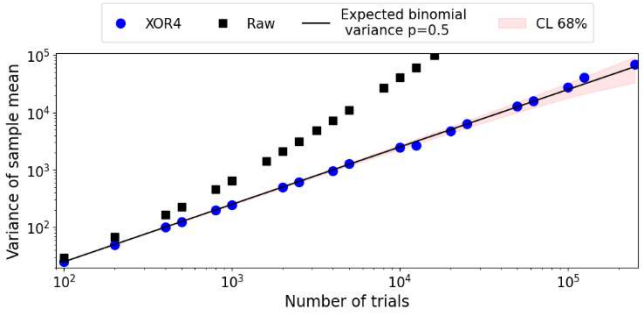

Fig. 4. Variance of the sample mean for sequential samples of XOR4 bitstreams. Each data point is extracted from the variance of the successful switching attempts histograms shown in Fig. 3.

TABLE I

Operation	Final entropy estimates (H)
Raw data	0.781805*
XOR2	0.981412
XOR4	0.995630
XOR8	0.995149

Final entropy estimates (H) from NIST entropy source validation, following the entropy estimation strategy from NIST SP 800-90B. *Raw data evaluated according to non-IID track.

REFERENCES

[1] K. Yang, et al. "16.3 A 23Mb/s 23pJ/b fully synthesized true-random-number generator in 28nm and 65nm CMOS," in 2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC), Feb. 2014, pp. 280–281.

[2] W. H. Choi *et al.*, "A Magnetic Tunnel Junction based True Random Number Generator with conditional perturb and real-time output probability tracking," in *2014 IEEE International Electron Devices Meeting*, Dec. 2014, p. 12.5.1-12.5.4.

[3] A. Fukushima *et al.*, "Spin dice: A scalable truly random number generator based on spintronics," *Appl. Phys. Express*, vol. 7, no. 8, p. 083001, Jul. 2014.

[4] H. Lee, F. Ebrahimi, P. K. Amiri, and K. L. Wang, "Design of high-throughput and low-power true random number generator utilizing perpendicularly magnetized voltage-controlled magnetic tunnel junction," *AIP Adv.*, vol. 7, no. 5, p. 055934, Mar. 2017.

[5] L. Rehm *et al.*, "Temperature-resilient random number generation with stochastic actuated magnetic tunnel junction devices," *Appl. Phys. Lett.*, vol. 124, no. 5, p. 052401, Jan. 2024.

[6] 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," in *2016 IEEE/ACM International Symposium on Nanoscale Architectures (NANOARCH)*, Jul. 2016, pp. 123–128.

[7] Y. Q. Xu *et al.*, "Self-stabilized true random number generator based on spin–orbit torque magnetic tunnel junctions without calibration," *Appl. Phys. Lett.*, vol. 125, no. 13, p. 132403, Sep. 2024.

[8] X. Chen, J. Zhang, and J. Xiao, "Magnetic-Tunnel-Junction-Based True Random-Number Generator with Enhanced Generation Rate," *Phys. Rev. Appl.*, vol. 18, no. 2, p. L021002, Aug. 2022.

[9] H. J. Ng, S. Yang, et al. "Provably Secure Randomness Generation from Switching Probability of Magnetic Tunnel Junctions," Phys. Rev. Appl., vol. 19, no. 3, p. 034077, Mar. 2023.

[10] L. Rehm et al., "Stochastic Magnetic Actuated Random Transducer Devices Based on Perpendicular Magnetic Tunnel Junctions," Phys. Rev. Appl., vol. 19, no. 2, p. 024035, Feb. 2023.

[11] L. Schnitzspan, et al. "Nanosecond True-Random-Number Generation with Superparamagnetic Tunnel Junctions: Identification of Joule Heating and Spin-Transfer-Torque Effects," Phys. Rev. Applied, vol. 20, no. 2, p. 024002, Aug. 2023.

[12] I. T. L. Computer Security Division, "Decision to Revise NIST SP 800-22 Rev. 1a | CSRC," CSRC | NIST. Accessed: May 22, 2025. [Online].

[13] M. Sönmez Turan, et al. "Recommendation for the Entropy Sources Used for Random Bit Generation," National Institute of Standards and Technology, NIST Special Publication (SP) 800-90B, Jan. 2018.