Stochastic Magnetic Actuated Random Transducer Devices Based on Perpendicular Magnetic Tunnel Junctions

L. Rehm,[1,*] C.C.M. Capriata,[1,2] S. Misra,[3] J.D. Smith,[3] M. Pinarbasi,[4] B.G. Malm,[2] and A.D. Kent[1,†]

[1] *Center for Quantum Phenomena, Department of Physics, New York University, New York, New York 10003, USA*
[2] *Division of Electronics and Embedded Systems, KTH Royal Institute of Technology, Stockholm 10044, Kingdom of Sweden*
[3] *Sandia National Laboratories, Albuquerque, New Mexico 87185, USA*
[4] *Spin Memory Inc., Fremont, California 94538, USA*

(Received 12 September 2022; revised 30 November 2022; accepted 12 January 2023; published 13 February 2023)

True random number generators are of great interest in many computing applications, such as cryptography, neuromorphic systems, and Monte Carlo simulations. Here, we investigate perpendicular magnetic-tunnel-junction nanopillars (pMTJs) activated by short-duration (nanosecond) pulses in the ballistic limit for such applications. In this limit, a pulse can transform the Boltzmann distribution of initial free-layer magnetization states into randomly magnetized down or up states, i.e., a bit that is 0 or 1, easily determined by measurement of the tunnel resistance of the junction. It is demonstrated that bit streams with millions of events: (1) are very well approximated by a normal distribution; (2) pass multiple statistical tests for true randomness, including all the National Institute of Standards and Technology tests for random number generators with only one XOR operation; (3) can be used to create a uniform distribution of 8-bit random numbers; and (4) can have no drift in the bit probability with time. The results presented here show that pMTJs operated in the ballistic regime can generate true random numbers at around 50-MHz bit rates, while being more robust to environmental changes, such as their operating temperature, compared to other stochastic nanomagnetic devices.

DOI: 10.1103/PhysRevApplied.19.024035

I. INTRODUCTION

True random number generators (TRNGs) are of great interest for many applications, such as cryptography [1], neuromorphic systems [2], and Monte Carlo simulations [3], which are extensively used to model and solve complex problems such as accurate climate models, biological processes, and particle production in high-energy colliders. There are TRNGs based on microscopic phenomena, such as thermal noise [4], quantum fluctuations [5]—such as radioactive decay [6]—and atmospheric environmental noise [7]. Nonetheless, an important goal remains the discovery and development of TRNG devices that are equally compact, fast, energy efficient, and robust with respect to device-to-device variability and environmental changes, such as their operating temperature.

Magnetic noise represents a new opportunity in this regard, as small ferromagnetic elements can be two-state systems, with their magnetization "up" and "down" states separated by an energy barrier E_b. If the energy barrier is comparable to the thermal energy kT, where k is the Boltzmann constant and T is the device operating temperature, the magnetization fluctuates between the two states, this being known as superparamagnetism. A magnetic-tunnel-junction (MTJ) device can convert these thermally driven magnetization fluctuations into two-level electrical signals that are easily read out and, further, MTJs are readily integrated with complementary metal-oxide semiconductor (CMOS) technology (see, e.g., Refs. [8–15]). In fact, MTJs with a superparamagnetic magnetic layer have already been explored for probabilistic computing [16–21]. However, these devices are either passive or driven by a constant bias and as a result their response depends strongly on the environmental noise. In the high-barrier limit ($E_b > kT$), their rate of fluctuations can be described by the Néel-Brown formula $\Gamma = \Gamma_0 \exp(-E_b/kT)$, where Γ_0 is the attempt frequency and is on the order of 1 GHz [22,23]. This indicates that the fluctuation rate is extremely (exponentially) sensitive to the temperature as well as changes in E_b associated with device and material parameter variations and external influences, such as magnetic fields.

Another phenomenon shown to be of interest for random number generation is the stochasticity of

*laura.rehm@nyu.edu
†andy.kent@nyu.edu

spin-transfer-torque (STT) switching of MTJs [24–27]. STT devices are conventionally used in memory applications, for which they are engineered to have two stable magnetic states [11,28,29]—high-energy barriers ($E_b > 60kT$)—but they also show great promise for this application [30] due to their small device footprint (≤ 20 nm) [31], energy efficiency (fJ), fast operation (subnanosecond), and controllability through their voltage bias or pulse time [32]. And, indeed, they have been investigated for TRNGs in the thermally assisted spin-transfer regime (long-pulse limit) [33,34] and with pulse durations approaching the thermally assisted spin-transfer regime [35]. Model studies of the use of voltage-controlled magnetic anisotropy to generate random bits have been reported [36–38] but device operation has not yet been explored. In the ballistic limit, the resulting junction state and thus the resulting bit (0 or 1) is random mainly because of the Boltzmann distribution of the initial magnetization states.

We denote this a stochastic magnetic actuated random transducer (SMART) device because the pulse activates the junction to generate a random bit stream, much like a coin flip. Figure 1(a) shows the Bloch sphere with an initial magnetization represented by a vector labeled $\hat{m}$. The blue and red shaded areas represent the thermal distribution of the initial magnetization states. The corresponding Boltzmann distribution of the initial magnetization z component (m_z) is represented on the right. After a pulse is applied, the blue regions will relax to $m_z = -1$ (switched, a bit 1) and the red to $m_z = +1$ (not switched, a bit 0), the initial magnetization state.

Here, we analyze and experimentally demonstrate the probabilistic behavior of medium-energy-barrier perpendicularly magnetized MTJs (pMTJs) in the ballistic limit. We show that the stochastic nature of the STT switching of these devices operating at a switching probability of 50% can be very well described by the statistics of Bernoulli trials. By whitening the experimentally obtained data stream with only one XOR operation [39], we fully pass the National Institute of Standards and Technology (NIST) statistical test suite for random number generators [40]. In addition, we use the same bit stream to generate a uniform distribution of random numbers, which is important for many applications.

II. SWITCHING PROBABILITY IN THE BALLISTIC LIMIT

Ballistic switching refers to the spin-torque-induced magnetization dynamics for short current or voltage pulses, typically on the order or less than a few nanoseconds. The main idea is that the pulse transfers angular momentum to the magnetic layer and there is no (or little) time for magnetic fluctuations during the pulse. The pulse can be considered to amplify the Boltzmann distribution of initial magnetization states, as shown schematically in Fig. 1(a). The switching probability in a macrospin model in the ballistic limit is given by [41–43]

$$p = \exp\left\{-\frac{\pi^2\Delta_{\text{eff}}}{4}\exp\left[-\left(\frac{V}{V_{c0}}-1\right)\frac{2\tau}{\tau_D}\right]\right\}, \quad (1)$$

where Δ_{eff} is the effective stability factor, which depends inversely on temperature and converges to $\Delta = E_b/(kT)$ in the very-short-duration–high-amplitude pulse limit. V_{c0} is the threshold bias, the switching threshold in the long-pulse limit, and τ is the applied-pulse duration. τ_D is the intrinsic time scale for the dynamics $\tau_D = (1+\alpha^2)/(\alpha\gamma\mu_0 H_k)$ [43], with α the damping constant, γ the gryomagnetic ratio, and μ_0 the permeability of free space. H_k is the anisotropy field: $H_k \equiv 2K_p/\mu_0 M_s - M_s$. Here, K_p is the perpendicular anisotropy and M_s is the saturation magnetization. Hence, τ_D is only indirectly dependent on temperature through changes in material parameters with temperature. The same is the case for V_{c0}, it depends on material parameters that are a function of temperature [44].

As we aim to operate the device near a switching probability p of 0.5, we derive an expression for the switching probability close to this value. With a linear approximation of Eq. (1) around $p = 0.5$ we find that

$$p(V) = \frac{1}{2} + \frac{\tau \ln 2}{\tau_D V_{c0}}(V - V_{1/2}), \quad (2)$$

$$V_{1/2} = V_{c0} + \frac{\tau_D V_{c0}}{2\tau}\ln\left(\frac{\pi^2\Delta_{\text{eff}}}{4\ln 2}\right), \quad (3)$$

where $V_{1/2}$ is the 50% switching-voltage threshold. Therefore, the switching voltage for $p = 0.5$ only depends logarithmically on temperature through Δ_{eff} and on material parameters V_{c0} and τ_D, which do not vary greatly with temperature (for device operation well below the Curie temperature of the magnet).

III. SMART-DEVICE CHARACTERISTICS

We conduct experiments in the ballistic limit on circularly shaped pMTJs with a MgO tunnel barrier. The free layer is a composite (Co-Fe-B)/W/(Co-Fe-B) layer stack (with composition Co-Fe-B $\equiv Co_{18}Fe_{54}B_{28}$) and the pinned layer is a Co-Fe-B layer that is ferromagnetically coupled to a synthetic antiferromagnet layer structure composed of two Pt/Co multilayers separated by a thin Ru layer. The room-temperature Δ of the pMTJs studied is 26 for the AP $\rightarrow$ P transition and 51 for the P $\rightarrow$ AP transition and the resistance-area product is $\simeq 3\ \Omega\ \mu m^2$ with a free-layer diameter of 40 nm. A more detailed description of the devices can be found in Refs. [32,44].

The stochastic write behavior of our SMART devices is studied by repeatedly applying a reset-read-write-read

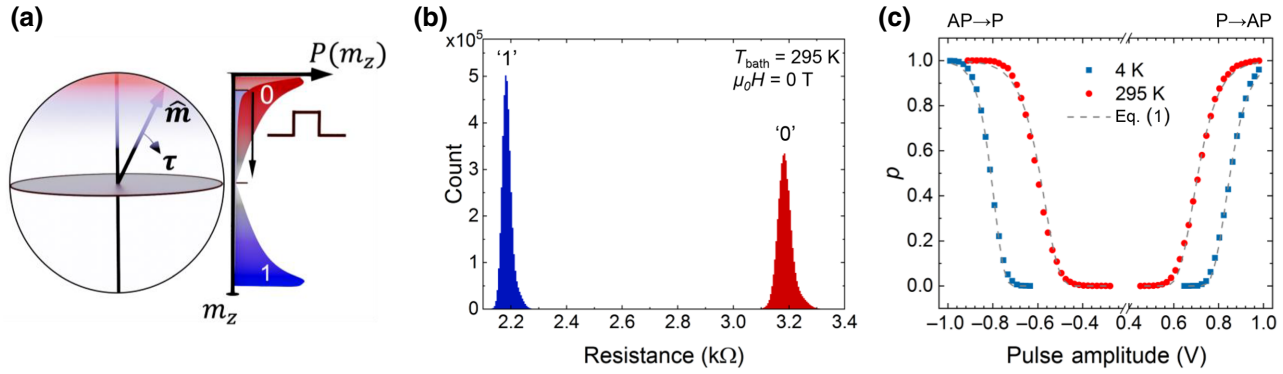

FIG. 1. Spin-transfer-torque switching in the ballistic regime. (a) A schematic of the Bloch sphere with an initial magnetization represented by a vector labeled $\hat{m}$ (left) and the initial thermal magnetization distribution indicated in light red and blue colors close to the north pole. After a current pulse, the z projection of the magnetization is bimodal, indicated schematically in dark red (0) and blue (1) on the right. (b) The histogram of the measured resistance values of a 40-nm-diameter pMTJ for 8×10^6 switching attempts with switching probability $p \approx 0.5$ for the AP $\rightarrow$ P transition at $T_{\text{bath}} = 295$ K and zero external field. The left peak corresponds to the resistance values where the device switches into P state (bit 1) and the right peak corresponds to the resistance values where the device remains in its initial AP state (bit 0). (c) The switching probability versus the pulse amplitude for a 1-ns-long pulse at 4 K (blue squares) and 295 K (red dots) with zero applied field. Each point is an average of 10 000 switching trials. The dashed gray curves show Eq. (1) plotted with experimental parameters determined as described in the main text.

scheme. We first reset to the desired state with a 50-μs-long pulse and pulse amplitudes well above the switching voltage (see Fig. 1(c) in the Supplemental Material [45]) and then we determine the state of the device before and after a 1-ns write pulse with a data acquisition (DAQ) board (National Instruments PCIe-6353). We choose a write pulse duration of 1 ns (Tektronix AWG 7102) as this is close to the most energy-efficient device-switching condition, corresponding to pulse times $\simeq \tau_D$. In addition, 1 ns is also optimal in terms of being the condition at which the switching probability is least sensitive to small variations in pulse duration and amplitude [32].

Figure 1(b) shows a histogram of the measured resistance values for 8×10^6 switching attempts obtained at room temperature ($T_{\text{bath}} = 295$ K) and zero external field. We can clearly observe two distinct well-separated resistance distributions corresponding to parallel- (P) and antiparallel- (AP) magnetization configurations with $\langle R_{\text{P}} \rangle$ and $\langle R_{\text{AP}} \rangle$ of 2180 and 3169 Ω, respectively. Based on the resistance distribution, we can then further evaluate if the resistance value obtained during the second read pulse falls into the criteria $\langle R_{\text{AP}} \rangle \pm 5 \times \sigma_{\text{AP}}$ or $\langle R_{\text{P}} \rangle \pm 5 \times \sigma_P$, where $\langle R \rangle$ is the mean of a resistance distribution and σ is its standard deviation. Thus, we assess if the device either switches or does not switch, assigning a 1 or 0, respectively. Additional device characterization can be found in Sec. 1 of the Supplemental Material [45].

IV. RESULTS AND ANALYSIS

Figure 1(c) shows the switching probability as a function of the pulse amplitude at room temperature (red dots). Each point on the graph represents $N_T = 10\,000$ switching attempts. As expected, the switching probability increases monotonically with the pulse amplitude. These data are analyzed with the ballistic macrospin model to obtain key device parameters. The variation of the switching probability with the pulse amplitude at $p = 1/2$, i.e., $dp/dV|_{p=1/2}$, gives $\tau_D V_{c0}$ [Eq. (2)] and the pulse amplitude to achieve $p = 0.5$ is $V_{1/2}$. V_{c0} is then determined using Eq. (3), assuming that Δ_{eff} is the thermal stability factor found in experiments with long-duration (> 10 μs) pulses (see Ref. [44]). With these parameters (i.e., V_{c0}, Δ_{eff}, and τ_D), the full curve for the switching probability versus the pulse amplitude [Eq. (1)] is plotted as gray dashed lines in Fig. 1(c). We find that these curves capture the characteristics of the experimental data well. In addition, we repeat the same measurements and analysis at low temperature, $T_{\text{bath}} = 4$ K [blue squares, Fig. 1(c)], to investigate the effect of a large change in temperature on the switching probability and fit parameters [46]. The experimentally determined parameters are given in Table I. Interestingly, $\tau_D V_{c0}$ does not change significantly with temperature, while V_{c0} depends more strongly on temperature. We use the junction material parameters to compute $\tau_D V_{c0}$ in the macrospin model and find that it is generally a factor of 3–8 larger than what is found experimentally (see Table I).

To further investigate the probabilistic behavior of our pMTJs, we increase the number of switching attempts N_T to 8×10^6 and focus on $p \simeq 0.5$. To analyze the switching statistics versus time and generate a switching probability distribution, we consider $N = 100$ nonoverlapping trials as samples. We then count the successfully switched attempts N_s in each sample (based on the criteria described earlier). The results for the AP $\rightarrow$ P transition at room temperature are shown in Fig. 2(a). The solid straight blue

TABLE I. Device parameters from experiment and a macrospin model. $\tau_D V_{c0}$ is obtained by fitting the probability versus pulse amplitude data as well as from the macrospin model. V_{c0} is determined using Eq. (3), taking Δ_{eff} from Ref. [44].

T (K)	Transition	Δ_{eff}	V_{c0} (V)	Fit: $\tau_D V_{c0}$ (sV)	Macrospin: $\tau_D V_{c0}$ (sV)
4	AP → P	129	−0.54	0.87×10^{-10}	6.9×10^{-10}
4	P → AP	129	0.51	1.11×10^{-10}	6.9×10^{-10}
295	AP → P	26	−0.32	1.27×10^{-10}	5.66×10^{-10}
295	P → AP	51	0.39	1.25×10^{-10}	5.66×10^{-10}

line represents the data set probability of $p = 0.5027$. We observe no drift. Figure 2(b) shows the histogram of a number of switching events; we observe a distribution that is symmetric around the mean.

Bernoulli trials describe a random event with two possible outcomes. Each trial is independent and the probability of the outcomes does not change over the trials. If the outcomes are "heads" and "tails" and the probability of "heads" is $p = 0.5$, then the Bernoulli trials describe flips of a fair coin. Letting p represent the probability of "success" and N represent the number of trials, for large N, the number of successes x is approximately normally distributed. The probability density function (PDF) for the number of successes is given by

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left\{ -\frac{(x-\mu)^2}{2\sigma^2} \right\}, \tag{4}$$

where $\mu = pN$ is the mean and $\sigma = \sqrt{N(1-p)}$ is the standard deviation. Returning to the pMTJs, of $N_T = 7\,999\,401$ total attempts, we find that 50.27% are bit flips. Using the Bernoulli-trial framework, our outcomes are whether or not a bit flip occurs and we take $p = 0.5027$. Then, for $N = 100$ trials, the expected mean number of bit flips is $\mu = 50.27$, with variance $\sigma^2 = 25.00$. The solid black line in Fig. 2(b) is a plot of the normal distribution [Eq. (4)] with these values; the histogram of our data is clearly very well characterized by this distribution function.

We continue by calculating the mean of the switched attempts $\mu = \langle N_s \rangle$ as well as the variance of the corresponding distribution as a function of N, the number of trials in a sample, with N varying from 10 to 2000:

$$\sigma^2 = \langle N_s^2 \rangle - \langle N_s \rangle^2. \tag{5}$$

This is shown in Fig. 2(c) as the red dots for the room-temperature data and the blue squares for data at 4 K. The solid black line represents the expected variance as a function of N for $p = 0.5$. The data deviates upward from the line at large sample size N, as expected when the number of total samples is not sufficiently large (i.e., when N approaches N_T).

V. SAMPLING A UNIFORM DISTRIBUTION

A critical elementary operation in probabilistic computing applications, e.g., Monte Carlo simulations, is to draw samples from different distributions. The fitness of different devices can be evaluated in terms of the statistical quality of the samples that their bit streams generate. We place eight consecutive readings of our SMART device in each position of an 8-bit string, interpreting it as a random number from 0 through 255. Figure 3(a) shows the histogram for 1 499 996 8-bit samples created from $N_T = 11\,999\,968$ measurements of the P → AP transition at $T_{\text{bath}} = 295$ K. The experimentally obtained random numbers (black data points) can be very well described by an ideal uniform distribution (red solid line) and provide a $\chi^2 = 1.13$.

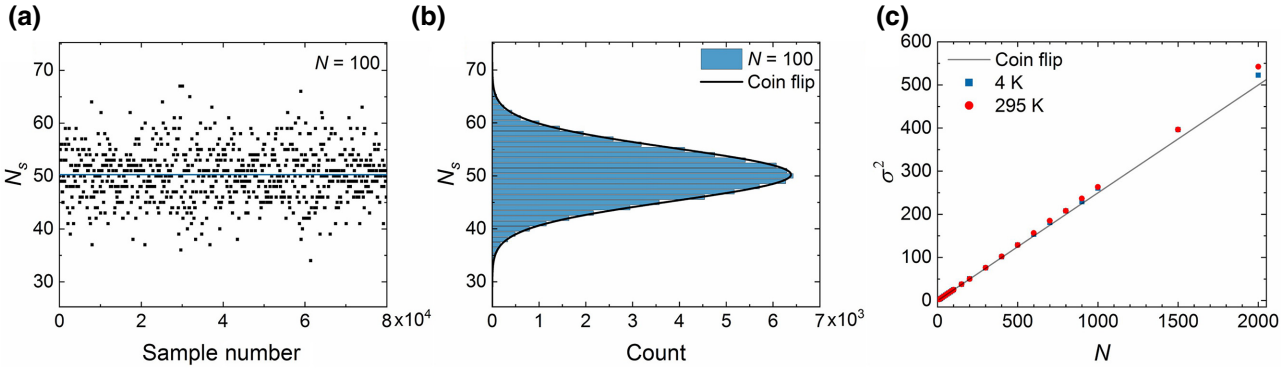

FIG. 2. Statistical analysis of the number of switched attempts. (a) The number of switched attempts N_s for the AP → P transition in a sample size of $N = 100$ versus the sample number for the same device at $T_{\text{bath}} = 295$ K. The solid straight line in the plot represents the switching probability $p = 0.5027$ of the whole data set ($N_T \approx 8 \times 10^6$). (b) The histogram of the switched events N_s of the same data set. The solid black line in the plot shows the normal distribution of a slightly weighted coin flip with a probability of $p = 0.5027$ and a variance of $\sigma^2 = 25.00$. (c) The variance σ^2 of the switched-attempts distribution versus the number of trials in a sample N at $T_{\text{bath}} = 4$ K (blue squares) and 295 K (red dots). The solid black line shows the expectation for a Bernoulli process with $p = 0.5$.

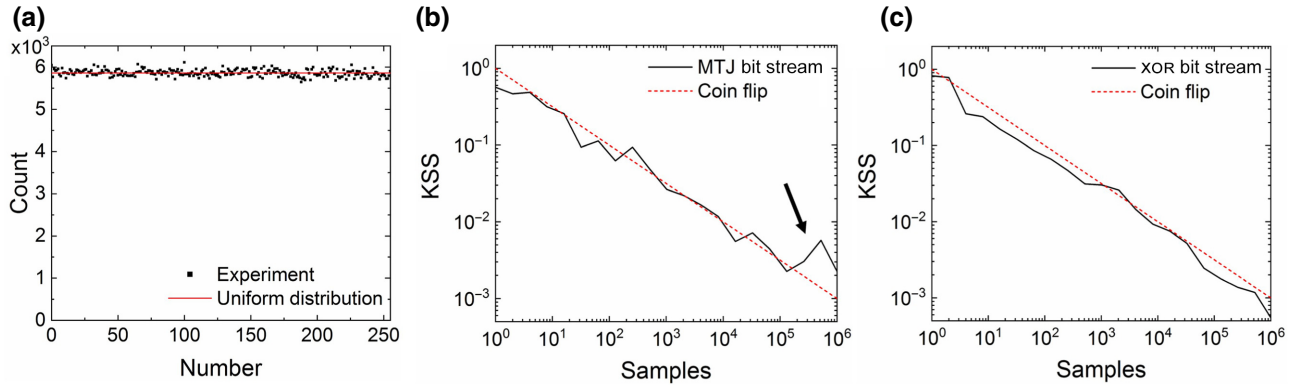

FIG. 3. Uniform distribution. (a) The 256-channel histogram of 1 499 996 8-bit values generated using the SMART bit stream. The histogram is fitted to a constant and provides a $\chi^2 = 1.13$. (b) The KSS versus the number of uniform samples for a bit stream generated using the pure bit stream (solid black line) and (c) the bit stream whitened by taking the XOR of consecutive bits (solid black line), with the dashed red line representing the result of an ideal distribution (coin flip) with KSS = $1/\sqrt{N}$. The black arrow in (b) shows where deviations from the ideal distribution occur due to small differences from $p = 0.5$.

The transformation of samples from a uniform distribution to various standard distributions and repeated calculations based on drawing many samples both rely on the quality of the uniform random samples generated. The use of a device that produces independent and identically distributed coin flips with $p = 0.5$ to generate an infinite number of uniform samples should yield a PDF that is a constant and a cumulative distribution function (CDF) that is a line with a constant slope. We quantify the error from a finite set of N samples using the Kolmogorov-Smirnov statistic (KSS), which measures the maximum deviation of the empirical CDF of the observed distribution from the desired distribution [47]. For a set of N uniform samples, the KSS $\sim 1/\sqrt{N}$ (Fig. 3(b), dashed red line). We now interpret the 8-bit string as a uniformly distributed random number [0,1) in 8-bit fixed-point notation. A plot of the KSS as a function of N uniform samples generated using the SMART bit stream, presented in Fig. 3(b), shows a deviation from $1/\sqrt{N}$ behavior for $N \sim 10^5$. This is a consequence of $p = 0.5 + \delta$ with $\delta = 2 \times 10^{-3}$ for this data set. Upon whitening the data by taking the logical XOR, exclusive or function, of consecutive bits [39], the error away from $p = 0.5$ is reduced to 4×10^{-4} and the KSS follows $1/\sqrt{N}$ to $N > 10^5$ [Fig. 3(c)]. More generally, any deviation from the desired p by δ will produce a lower limit beyond which increased sampling will not improve the KSS beyond order δ. Heuristically, there is a limit to the number of samples we can take while ignoring the small deviation from a fair flip. This derives from the deviation in the probability of most 8-bit strings being of order δ, with the deviation being positive if the number of ones is more than the number of zeros, vice versa, and zero if they are equal. Put differently, the number of samples beyond which deviation of the generated samples from the desired distribution becomes statistically significant is of order $1/\delta^2$.

We close this discussion by emphasizing that there are other characteristics of the SMART bit stream, such as an absence of correlations and timing that indicates random draws, which lead to the relationship of p and the KSS. In devices where those pathologies are present, even if they more faithfully produce $p = 0.5$, limitations to the quality of the samples will simply have a different origin. Analysis of these connections is provided in greater detail in Sec. II of the Supplemental Material [45].

VI. NIST STATISTICAL TESTS

In addition to the statistical analysis of the STT switching of our pMTJs and the generation of uniform random numbers, we also test the generated data streams with the NIST statistical test suite [40]. The test suite consists of numerous frequency- and nonfrequency-related tests. The frequency-related tests evaluate the number of ones in the data set, while the nonfrequency-related tests check, for example, for special patterns. The results of a $N_T = 12$M data stream can be found in Table II.

We find that our initial data streams obtained at room temperature for the AP $\rightarrow$ P transition with $p = 0.5027$ and P $\rightarrow$ AP with $p = 0.5034$ pass 184 out of the 188 tests, resulting in an identical passing rate of 97.87% (see XOR stage 0 in Table II). We whiten the bit stream with a single XOR operation and the effect of this process is again evident: the passing rate jumps to 100%—all tests pass (see XOR stage 1 in Table II). While we are creating the bit streams from a single device, it is clearly possible to parallelize the creation of the inputs by simply using multiple devices that will result in a reduction of the probability bias of the order δ to δ^2, assuming identical device-switching probabilities (for more detailed information about the NIST tests, see Sec. 3 in the Supplemental Material [45]).

TABLE II. NIST test results of the SMART bit streams: the whitened bit streams after one and two XOR operations.

	AP → P			P → AP		
Test name / XOR stages	0	1	2	0	1	2
Frequency (monobit)	0/1	1/1	1/1	0/1	1/1	1/1
Frequency within a block	1/1	1/1	1/1	1/1	1/1	1/1
Run	0/1	1/1	1/1	1/1	1/1	1/1
Longest run of ones in a block	1/1	1/1	1/1	1/1	1/1	1/1
Binary matrix rank	1/1	1/1	1/1	1/1	1/1	1/1
Discrete Fourier transform (spectral)	1/1	1/1	1/1	1/1	1/1	1/1
Nonoverlapping template matching	148/148	148/148	148/148	147/148	148/148	148/148
Overlapping template matching	1/1	1/1	1/1	1/1	1/1	1/1
Maurer's universal statistic	1/1	1/1	1/1	1/1	1/1	1/1
Linear complexity	1/1	1/1	1/1	1/1	1/1	1/1
Serial	2/2	2/2	2/2	2/2	2/2	2/2
Approximate entropy	1/1	1/1	1/1	1/1	1/1	1/1
Cumulative sums (forward)	0/1	1/1	1/1	0/1	1/1	1/1
Cumulative sums (reverse)	0/1	1/1	1/1	0/1	1/1	1/1
Random excursions	8/8	8/8	8/8	8/8	8/8	8/8
Random excursions variant	18/18	18/18	18/18	18/18	18/18	18/18

VII. DISCUSSION

We see that the small probability bias of our SMART device can be handled by whitening the bit stream but it can also be managed by simply adjusting the pulse amplitude or pulse duration. In devices integrated with CMOS, the access transistor enables individual device programming and sample-to-sample variations will require an array calibration step. This can be used to determine $V_{1/2}$ for each device and the resulting calibration table used for chip operation. While the whitening of the bit stream is generally a great way to improve the quality of the random numbers, adjusting the pulse condition can only be used for a fixed (time-independent) deviation of the switching probability from 0.5.

We expect our SMART devices to be relatively insensitive to changes in operating temperature. For instance, a temperature change of ± 2.95 K would change Δ by ±1% and results in a change of $p \pm 0.35\%$ in the ballistic limit [Eq. (2)]. However, for long pulses (i.e., $\tau \gg \tau_D$), the spin torque can be considered to modify the energy barrier to thermally activated reversal. Fukushima *et al.* [34] assume $p = 1 - \exp(-\Gamma_0 \tau \exp(-\Delta(1-v)^{\nu}))$, with $\nu = 2$. Due to this double-exponential temperature dependence, the same change in Δ of ±1% would lead to $p \pm 5.03\%$ (taking the device parameters from Ref. [34], $\Delta = 109$, $\Gamma_0 = 10^9$ s^{-1}, $\tau = 200$ ns, $v = 0.76$). The same double-exponential temperature dependence can be found for the switching probability of superparamagnetic MTJs, where $p(t) = 1 - \exp(-\Gamma_0 t \exp(-\Delta))$ with t being the read time. With $t = 604$ μs from Ref. [16], this would lead to $p \pm 16.41\%$ for the superparamagnetic MTJs, which is thus very sensitive to small changes in temperature compared to the switching probability of our SMART devices.

A comparison of the key characteristics of MTJ-based devices for TRNG can be found in Table III, with the devices included and parameters based on experimental studies. The SMART-device cycle to obtain a single random bit consists of a 1-ns write, a 10-ns read, and a 5-ns reset pulse, with a 2-ns wait period between the write and read operations, giving a random bit rate of $\simeq 50$ MHz. This timing cycle is also used to estimate the energy required per random bit in Table III.

We now return to the device parameters in Table I. As noted earlier, we find that the fit values of $\tau_D V_{c0}$ are smaller than those expected based on the macrospin model with

TABLE III. A comparison of the key performance criteria of MTJ-based TRNG devices operated at room temperature. The energy per bit corresponds to the energy cost needed to create a single random bit. The quality of the randomness described by XORn stands for how many XOR combined bit streams n are needed to pass the NIST tests. The temperature sensitivity shows the percentage change in p for a 2.95 K (1 %) variation in temperature with the device operating at room temperature and the device characteristics taken from the references shown at the top of each column.

MTJ device concepts	Superparamagnetic (Ref. [16])	Thermally assisted regime (Ref. [34])	SMART (this work)
Bitrate (Mbit/s)	0.005	0.6	50
Energy per bit (fJ)	2	22 600	292
Quality of randomness	XOR8	XOR4	XOR2
Temperature sensitivity	16.41%	5.03%	0.35%

our device material parameters. This is consistent with other experiments on nanomagnetic switching dynamics that find shorter time scales τ_D than those in the macrospin model [48,49]. Further, the change in V_{c0} from $T_{\text{bath}} = 295$ to 4 K is similar to the percentage changes that we find in V_{c0} in this temperature range by analyzing long-duration pulse results (see Fig. 3(a) of Ref. [44]).

VIII. CONCLUSIONS

In summary, these results clearly demonstrate that medium-energy-barrier pMTJs operating in the ballistic limit have great potential for true random number generation. We assess the statistics of the experimentally obtained bit streams by comparing them to a normal distribution as well as exploring their potential for numerous applications by sampling a uniform distribution. By whitening the bit stream with one XOR operation, we show that the bit stream passes all NIST tests designed for evaluating the quality of random number generators. In addition, compared to other nanomagnetic device concepts, such as STT devices operated with long-duration pulses and superparamagnetic MTJs, we find that our devices show the potential of a lower sensitivity to temperature variations, can have no drift of the switching probability with time, and offer the possibility of precisely varying the switching probability through the pulse conditions.

ACKNOWLEDGMENTS

This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government. Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under Contract No. DE-NA0003525. We acknowledge support from the DOE Office of Science (Advanced Scientific Computing Research (ASCR) and Basic Energy Sciences (BES)) Microelectronics Co-Design project COINFLIPS. We thank Shaloo Rakheja and Avik Ghosh for discussions of the ballistic macrospin model and Spin Memory for providing the magnetic tunnel junctions. We especially thank Bartek Kardasz for the layer stack deposition and characterization and Georg Wolf for the initial device screening. We would also like to thank Guanzhong Wu for his assistance in creating Fig. 1(a). This work was partially supported by the Swedish Research Council (VR), project Fundamental Fluctuations in Spintronics, 2017-04196. We also thank the funding agencies Nils and Hans Backmark Foundation (J-2021-2437) and Karl Engvers Foundation for supporting the project. This work was also partly funded under the Laboratory Directed Research and Development program at Sandia National Laboratories.

[1] J. L. McInnes and B. Pinkas, in *Advances in Cryptology-CRYPTO' 90*, edited by A. J. Menezes and S. A. Vanstone (Springer-Verlag, Berlin, 1991), p. 421.

[2] C. D. Schuman, T. E. Potok, R. M. Patton, J. D. Birdwell, M. E. Dean, G. S. Rose, and J. S. Plank, A Survey of Neuromorphic Computing and Neural Networks in Hardware, CoRR **abs/1705.06963** (2017).

[3] R. L. Harrison, Introduction to Monte Carlo simulation, AIP Conf. Proc. **1204**, 17 (2010).

[4] H. Zhun and C. Hongyi, in *ASICON 2001. 2001 4th International Conference on ASIC Proceedings (Cat. No.01TH8549)* (IEEE, Shanghai, China, 2001), p. 862.

[5] M. Herrero-Collantes and J. C. Garcia-Escartin, Quantum random number generators, Rev. Mod. Phys. **89**, 015004 (2017).

[6] M. Rohe *et al.*, in *RANDy—A true-random generator based on radioactive decay* (Saarbrücken: Fortgeschrittenenpraktikum, Security and Cryptography Research Group Saarland University, 2003), p. 1.

[7] D. Kumar, C. D. Jadhav, P. K. Misra, and M. Goswami, in *2020 24th International Symposium on VLSI Design and Test (VDAT)* (IEEE, Bhubaneswar, India, 2020), p. 1.

[8] G. Prenat, M. El Baraji, W. Guo, R. Sousa, L. Buda-Prejbeanu, B. Dieny, V. Javerliac, J.-P. Nozieres, W. Zhao, and E. Belhaire, in *2007 14th IEEE International Conference on Electronics, Circuits and Systems* (IEEE, Marrakech, Morocco, 2007), p. 190.

[9] S. Matsunaga, J. Hayakawa, S. Ikeda, K. Miura, H. Hasegawa, T. Endoh, H. Ohno, and T. Hanyu, Fabrication of a nonvolatile full adder based on logic-in-memory architecture using magnetic tunnel junctions, Appl. Phys. Express **1**, 091301 (2008).

[10] W. Zhao, E. Belhaire, C. Chappert, F. Jacquet, and P. Mazoyer, New non-volatile logic based on spin-MTJ, Phys. Status Solidi (a) **205**, 1373 (2008).

[11] A. D. Kent and D. C. Worledge, A new spin on magnetic memories, Nat. Nanotechnol. **10**, 187 (2015).

[12] E. Deng, G. Prenat, L. Anghel, and W. Zhao, Non-volatile magnetic decoder based on MTJs, Electron. Lett. **52**, 1774 (2016).

[13] S. D. Kumar and H. Thapliyal, Exploration of non-volatile MTJ/CMOS circuits for DPA-resistant embedded hardware, IEEE Trans. Magn. **55**, 1 (2019).

[14] P. Barla, V. K. Joshi, and S. Bhat, A novel low power and reduced transistor count magnetic arithmetic logic unit using hybrid STT-MTJ/CMOS circuit, IEEE Access **8**, 6876 (2020).

[15] P. Barla, D. Shet, V. K. Joshi, and S. Bhat, in *2020 5th International Conference on Devices, Circuits and Systems (ICDCS)* (IEEE, Coimbatore, India, 2020), p. 41.

[16] D. Vodenicarevic, N. Locatelli, A. Mizrahi, J. S. Friedman, A. F. Vincent, M. Romera, A. Fukushima, K. Yakushiji, H. Kubota, S. Yuasa, S. Tiwari, J. Grollier, and D. Querlioz, Low-Energy Truly Random Number Generation with Superparamagnetic Tunnel Junctions for

Unconventional Computing, Phys. Rev. Appl. **8**, 054045 (2017).
[17] W. A. Borders, A. Z. Pervaiz, S. Fukami, K. Y. Camsari, H. Ohno, and S. Datta, Integer factorization using stochastic magnetic tunnel junctions, Nature **573**, 390 (2019).
[18] J. Kaiser, A. Rustagi, K. Y. Camsari, J. Z. Sun, S. Datta, and P. Upadhyaya, Subnanosecond Fluctuations in Low-Barrier Nanomagnets, Phys. Rev. Appl. **12**, 054056 (2019).
[19] K. Hayakawa, S. Kanai, T. Funatsu, J. Igarashi, B. Jinnai, W. A. Borders, H. Ohno, and S. Fukami, Nanosecond Random Telegraph Noise in In-Plane Magnetic Tunnel Junctions, Phys. Rev. Lett. **126**, 117202 (2021).
[20] C. Safranski, J. Kaiser, P. Trouilloud, P. Hashemi, G. Hu, and J. Z. Sun, Demonstration of nanosecond operation in stochastic magnetic tunnel junctions, Nano Lett. **21**, 2040 (2021).
[21] B. Parks, M. Bapna, J. Igbokwe, H. Almasi, W. Wang, and S. A. Majetich, Superparamagnetic perpendicular magnetic tunnel junctions for true random number generators, AIP Adv. **8**, 055903 (2018).
[22] L. Néel, Théorie du traînage magnétique des ferromagnétiques en grains fins avec application aux terres cuites, Ann. Géophys. **5**, 99 (1949).
[23] W. F. Brown, Thermal fluctuations of a single-domain particle, Phys. Rev. **130**, 1677 (1963).
[24] J. Slonczewski, Current-driven excitation of magnetic multilayers, J. Magn. Magn. Mater. **159**, L1 (1996).
[25] L. Berger, Emission of spin waves by a magnetic multilayer traversed by a current, Phys. Rev. B **54**, 9353 (1996).
[26] G. Bertotti, I. D. Mayergoyz, and C. Serpico, in *Nonlinear Magnetization Dynamics in Nanosystems*, Elsevier Series in Electromagnetism, edited by G. Bertotti, I. D. Mayergoyz, and C. Serpico (Elsevier, Oxford, 2009), p. 271.
[27] F. J. Albert, N. C. Emley, E. B. Myers, D. C. Ralph, and R. A. Buhrman, Quantitative Study of Magnetization Reversal by Spin-Polarized Current in Magnetic Multilayer Nanopillars, Phys. Rev. Lett. **89**, 226802 (2002).
[28] J. M. Slaughter, N. D. Rizzo, J. Janesky, R. Whig, F. B. Mancoff, D. Houssameddine, J. J. Sun, S. Aggarwal, K. Nagel, S. A. Deshpande, S. M. Alam, T. W. Andre, and P. LoPresti, High density ST-MRAM technology, 2012 International Electron Devices Meeting, 29.3.1 (2012).
[29] L. Thomas, G. Jan, S. Le, Y. Lee, H. Liu, J. Zhu, S. Serrano-Guisan, R. Tong, K. Pi, D. Shen, R. He, J. Haq, Z. Teng, R. Annapragada, V. Lam, Y. Wang, T. Zhong, T. Torng, and P. Wang, in *2015 IEEE International Electron Devices Meeting (IEDM)* (IEEE, Washington, DC, USA, 2015), p. 26.4.1.
[30] S. Misra, L. C. Bland, S. G. Cardwell, J. A. C. Incorvia, C. D. James, A. D. Kent, C. D. Schuman, J. D. Smith, and J. B. Aimone, Probabilistic neural computing with stochastic devices, Adv. Mater. **n/a**, 2204569 (2022).
[31] B. Jinnai, J. Igarashi, T. Shinoda, K. Watanabe, S. Fukami, and H. Ohno, in *2021 IEEE International Electron Devices Meeting (IEDM)* (IEEE, San Francisco, CA, USA, 2021), p. 1.
[32] L. Rehm, G. Wolf, B. Kardasz, M. Pinarbasi, and A. D. Kent, Sub-nanosecond spin-torque switching of perpendicular magnetic tunnel junction nanopillars at cryogenic temperatures, Appl. Phys. Lett. **115**, 182404 (2019).
[33] S. Yuasa *et al.*, in *2013 IEEE International Electron Devices Meeting* (IEEE, Washington, DC, USA, 2013), p. 3.1.1.
[34] 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 **7**, 083001 (2014).
[35] W. H. Choi, Y. Lv, J. Kim, A. Deshpande, G. Kang, J.-P. Wang, and C. H. Kim, in *2014 IEEE International Electron Devices Meeting* (IEEE, San Francisco, CA, USA, 2014), p. 12–5.
[36] A. Sengupta, A. Jaiswal, and K. Roy, in *2016 74th Annual Device Research Conference (DRC)* (IEEE, Newark, DE, USA, 2016), p. 1.
[37] 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. **7**, 055934 (2017).
[38] L. R. A. Quizon, A. B. Alvarez, C. G. Santos, M. D. Rosales, J. R. E. Hizon, M. P. Rouelli, and G. Sabino, in *2021 18th International SoC Design Conference (ISOCC)* (IEEE, Jeju Island, Korea, 2021), p. 159.
[39] M. Matsui, in *Advances in Cryptology—EUROCRYPT '93*, edited by T. Helleseth (Springer-Verlag, Berlin, 1994), p. 386.
[40] L. E. Bassham III, A. Rukhin, J. Soto, J. Nechvatal, M. Smid, S. Leigh, M. Levenson, M. Vangel, N. Heckert, and D. Banks, Sp 800–22 Rev. 1a, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, National Institute of Standards &Technology (2010), https://www.nist.gov/publications/statistical-test-suite-random-and-pseudorandom-number-generators-cryptographic.
[41] W. H. Butler, T. Mewes, C. K. A. Mewes, P. B. Visscher, W. H. Rippard, S. E. Russek, and R. Heindl, Switching distributions for perpendicular spin-torque devices within the macrospin approximation, IEEE. Trans. Magn. **48**, 4684 (2012).
[42] K. Munira, W. H. Butler, and A. W. Ghosh, A quasi-analytical model for energy-delay-reliability tradeoff studies during write operations in a perpendicular STT-RAM cell, IEEE Trans. Electron Devices **59**, 2221 (2012).
[43] H. Liu, D. Bedau, J. Sun, S. Mangin, E. Fullerton, J. Katine, and A. Kent, Dynamics of spin torque switching in all-perpendicular spin valve nanopillars, J. Magn. Magn. Mater. **358-359**, 233 (2014).
[44] L. Rehm, G. Wolf, B. Kardasz, E. Cogulu, Y. Chen, M. Pinarbasi, and A. D. Kent, Thermal Effects in Spin-Torque Switching of Perpendicular Magnetic Tunnel Junctions at Cryogenic Temperatures, Phys. Rev. Appl. **15**, 034088 (2021).
[45] See the Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevApplied.19.024035 for more information about the device characterization and more characteristics of the SMART bit stream, as well as the NIST test. (2022).

[46] It should be noted during pulses, the temperature of the device can be significantly greater than the bath temperature due to junction heating [44].
[47] O. Thas, *Comparing Distributions* (Springer, New York, 2010), Vol. 233, p. 297.
[48] S. Krause, G. Herzog, T. Stapelfeldt, L. Berbil-Bautista, M. Bode, E. Y. Vedmedenko, and R. Wiesendanger, Magnetization Reversal of Nanoscale Islands: How Size and Shape Affect the Arrhenius Prefactor, Phys. Rev. Lett. **103**, 127202 (2009).
[49] D. Bedau, H. Liu, J. Z. Sun, J. A. Katine, E. E. Fullerton, S. Mangin, and A. D. Kent, Spin-transfer pulse switching: From the dynamic to the thermally activated regime, Appl. Phys. Lett. **97**, 262502 (2010).