FerroCoin: Ferroelectric Tunnel Junction-based True Random Number Generator

Swetaki Chatterjee, *Student Member, IEEE,* Nikhil Rangarajan, *Member, IEEE,* Satwik Patnaik, *Member, IEEE,* Dinesh Rajasekharan, *Member, IEEE,* Ozgur Sinanoglu, *Senior Member, IEEE,* and Yogesh Singh Chauhan, *Fellow, IEEE*

Abstract—In this paper, we propose a Ferroelectric Tunnel Junction (FTJ)-based true random number generator (TRNG) that utilizes the stochastic domain switching phenomenon in ferroelectric materials. Ferroelectrics are promising for extracting randomness owing to their innate switching entropy in the multi-domain state. The random numbers generated by the proposed TRNG are shown to pass all the NIST SP 800-22 tests. The robustness of the proposed TRNG is also validated at various temperature and process corners. Important metrics such as power, bit rate, and energy/bit are calculated. This is the first comprehensive work demonstrating a ferroelectric-based TRNG with all these metrics. Compared to state-of-the-art TRNGs using other emerging technologies, we can achieve a higher bit rate with lower power consumption. We also perform material-level optimization with different ferroelectric materials, and showcase the trade-off between the bit rate and the power consumption. The proposed TRNG shows high robustness and reliability, and thus has the potential for implementing a low power on-chip solution.

Index Terms—Hardware Security, True Random Number Generator, Ferroelectric Tunnel Junction, Stochasticity, Domain Switching

1 Introduction

Random numbers are an integral part of many real-world applications ranging from cryptography, graphics design, artificial intelligence, and hardware security [1]. This calls for a high degree of randomness in the numbers generated which is only possible from a physical source of entropy. Software-based pseudo random number generators (PRNG) are not suitable for this purpose. This warrants the need for true random number generators (TRNGs) harnessing some form of stochasticity. However, traditional CMOS-based TRNGs have high power consumption and are not suitable for resource-constrained future edge computing [2]. Also, CMOS-based TRNGs require huge post-processing to generate truly random bits, which exacerbates the overheads. This necessitates the development of emerging technology-based TRNGs, which can generate random numbers at high bit rates and at a fraction of the power. In this regard, many emerging technology-based TRNGs have been proposed. Some of them are discussed in the following section.

1.1 Prior Work

The precessional switching of nanomagnets is used as a source of entropy in [3]. Variations of the read and write current in resistive random access memory (RRAM)-based devices have been leveraged to build a TRNG in [4]. Read noise in Flash memory cells has also been demonstrated as a source of entropy for Flash-based TRNGs [5]. However, both implementations [4], [5] are unreliable and there is a huge variation in the states which often leads to skewed distribution in the probability of either 1 or 0. Recently, programming stochasticity in atomically thin 2-D material based transistors has been exploited to design a TRNG [6]. However, its high energy/bit (10 pJ) compared to the existing state-of-the-art prohibits its use. Another interesting approach is presented in [7], where the authors propose a TRNG based on stochastic switching of the magnetic tunnel junctions (MTJ) in subcritical current regime within a neuromorphic framework. This leads to a highly stable and low power solution but the complex architecture and huge area of the design is a major hindrance for its practical use on chip. A promising TRNG is proposed in [8] that exploits the stochastic switching in memristors which has a very high bit rate and an extremely low power consumption. However, no standardized statistical tests have been performed to evaluate the entropy of the output bits. Also, this design requires significant post-processing and precise control of the programming criterion.

Variation in the switching time of ferroelectrics in ferroelectric field effect transistor (FeFET) has been showcased before [9]. However, the authors in [9] have not quantified important metrics such as degree of randomness, power and area. In this paper, we present *FerroCoin*, a ferroelectric tunnel junction (FTJ)-based TRNG. To our knowledge, this is the first TRNG built using FTJs, with a comprehensive analysis of performance metrics, benchmarking, and comparison with prior state-of-the-art. *FerroCoin* leverages the principle of stochastic domain nucleation time in ferroelectric materials [10]. The time period of applied pulses is adjusted

- *Swetaki Chatterjee and Yogesh Singh Chauhan are with the Department of Electrical Engineering, Indian Institute of Technology Kanpur, Kanpur 208016 India (e-mail: swetakic@iitk.ac.in; chauhan@iitk.ac.in).*
- *Nikhil Rangarajan and Ozgur Sinanoglu are with the Division of Engineering, New York University Abu Dhabi, Abu Dhabi, 129188 UAE (e-mail: nikhil.rangarajan@nyu.edu; ozgursin@nyu.edu).*
- *Satwik Patnaik is with the Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843 USA (e-mail: satwik.patnaik@tamu.edu).*
- *Dinesh Rajasekharan is with the Department of Electrical Engineering and Computer Science, University of California at Berkeley, Berkeley, CA 94720 USA.*

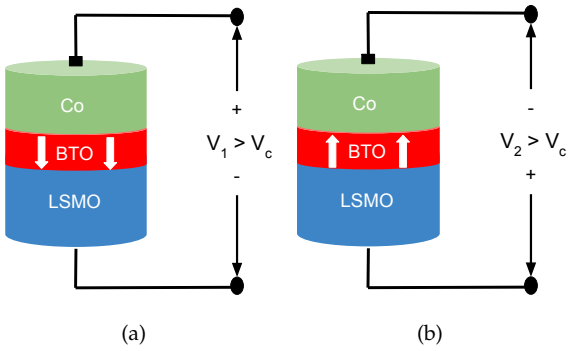


Fig. 1: A representative diagram of the FTJ device constructed with $Co/BaTiO_3$ (BTO)/$La_{0.67}Sr_{0.33}MnO_3$ (LSMO), showing polarization in (a) down direction and (b) up direction

such that the probability of switching stays at 50%, leading to equiprobable high and low states. Further, *FerroCoin* performs better than most of the prior implementations in the literature in terms of bit-rate and entropy, at a fraction of the power, and does not require any post-processing of the output bits.

This paper is organized as follows. Section 2 presents a background on the working and modeling of FTJs. Section 3 highlights the entropy source of the *FerroCoin*, i.e, the randomness in the switching of the ferroelectric domains. In section 4, the detailed working of *FerroCoin* is elucidated, followed by the security analysis in section 5. Finally, section 6 details the performance evaluation of *FerroCoin*, and provides benchmarking with state-of-the-art implementations.

2 Ferroelectric Tunnel Junction

The ferroelectric tunnel junction (FTJ) is a 2-terminal structure that has an ultrathin ferroelectric barrier layer sandwiched between two different metals as shown in Fig. 1. The ferroelectric tunnel barrier exists in two stable spontaneous polarization states. The tunneling current flowing through the FTJ is different in the two states. Thus, the tunneling electro-resistance (TER) in both states is different and enables the FTJ to be used as a non-volatile memory (NVM). An external voltage larger than the coercive voltage (V_c) is able to switch the state of polarization. Compared to magnetic tunnel junctions (MTJ) the on-off ratio is much higher in FTJ, with lower requirements for the write voltage [11].

2.1 FTJ Construction and Working

The FTJ device considered for this work is shown in Fig. 1. The FTJ stack is made of $Co/BaTiO_3/La_{0.67}Sr_{0.33}MnO_3$. The ferroelectric $BaTiO_3$ (BTO) layer shows spontaneous polarization depending on the displacement of the cation (Ti^{4+}) from its centrosymmetric position. The two different polarization states cause a difference in the barrier potential at the metal/ferroelectric interface due to asymmetric charge screening. Consequently, the current flowing through the two states is different as the probability of electron tunneling through the barrier depends on the height of barrier potential [12]. The high resistance state (HRS) corresponds to the OFF state wherein the barrier height is high, and low resistance state (LRS) corresponds to the ON state wherein the barrier height is low. The switching between these two states is a voltage-dependent phenomenon.

The switching from one equilibrium state to the other in scaled FTJs occurs via domain nucleation and domain wall propagation. A domain is a region in the ferroelectric layer where all the dipoles have the same polarization direction. On applying a voltage greater than the coercive voltage, a small fraction of the domains flip their polarization, which is called nucleation. This is followed by sideways and forward growth of the domain, called domain wall propagation. Thus, switching from one state to another is a gradual process and does not occur abruptly. This determines the characteristic switching time of the FTJ. It has been reported in the literature and confirmed experimentally that the domain nucleation is a stochastic process [10]. Thus, the switching time of FTJs is a stochastic quantity.

In this work, we consider a 2 nm thick BTO layer for our analysis. The area of the FTJ device is 0.096 μm^2. Note that the thickness of the barrier layer is less than the critical thickness for the devices to show tunneling.

2.2 FTJ Modeling

The FTJ used in this work is modeled as in [13], using *Verilog-A*, and has been simulated in *Cadence SPECTRE*. The bias-dependent tunnel resistance at low readout voltages is expressed using the Brinkman Model [14] as

$$R(0) = \left.\frac{dV}{dI}\right|_{V=0} = \frac{2\sqrt{2}\pi^2\hbar}{e^2 A}\cdot\frac{t_B}{\bar{\varphi}^{1/2}\cdot S}\exp\left(2\sqrt{2}A\cdot t_B\cdot\bar{\varphi}^{1/2}\right), \tag{1}$$

$$R_{\text{diff}}(V) = \frac{dV}{dI} = \frac{R(0)}{1-\frac{\sqrt{2}}{12}\cdot\frac{A\cdot t_B\cdot\Delta\varphi}{\bar{\varphi}^{3/2}}\cdot V+\frac{1}{4}\cdot\frac{A^2 t_B^2}{\bar{\varphi}}\cdot V^2}, \tag{2}$$

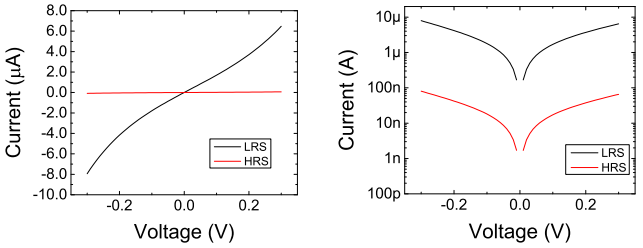
where $A = \frac{\sqrt{me}}{\hbar}$, R(0) is the resistance under zero bias voltage, I is the current, t_B is the barrier thickness, S is the surface area of the device, $\bar{\varphi}$ is the average barrier potential height, and $\Delta\varphi$ is the difference in the barrier potential height between two metal/insulator boundaries. The I-V curve of the FTJ can be derived from eq. (2). However, a better approximation of the I-V characteristics is given by the Gruverman [15] model, which uses more realistic parameters for the FTJ. In the low voltage regime, where direct tunneling (DT) is dominant, the I-V relationship can be approximated as

$$I(V) = S\cdot C\frac{\exp\left\{\alpha(V)\left[\left(\varphi_2-\frac{V}{2}\right)^{3/2}-\left(\varphi_1+\frac{V}{2}\right)^{3/2}\right]\right\}}{\alpha^2(V)\left[\left(\varphi_2-\frac{V}{2}\right)^{1/2}-\left(\varphi_1+\frac{V}{2}\right)^{1/2}\right]^2}$$
$$\times\sinh\left\{\frac{3}{2}\alpha(V)\left[\left(\varphi_2-\frac{V}{2}\right)^{1/2}-\left(\varphi_1+\frac{V}{2}\right)^{1/2}\right]\frac{V}{2}\right\}, \tag{3}$$

where

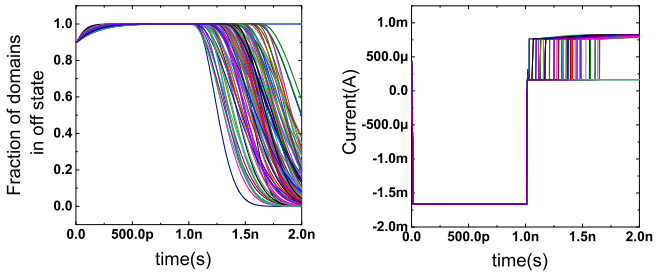
$$C = \frac{4me^3}{9\pi^2\hbar^3},\ \alpha(V) = \frac{4t_B(2m_e)^{1/2}}{3\hbar(\varphi_1+V-\varphi_2)},$$

m_e is the free electron mass and m is the effective electron mass inside the barrier, which has been shown to be differ-



(a) (b)

Fig. 2: I-V characteristics of the simulated FTJ showing I_{on}/I_{off} ratio of ~100 in (a) linear scale and (b) logarithmic scale



(a) (b)

Fig. 3: Switching characteristics of the FTJ showing (a) the fraction of domains switched versus time and (b) the current in the FTJ versus time

ent in different materials and also in different states. φ_1 and φ_2 are potential barrier heights at LSMO/BTO and Co/BTO interfaces, respectively.

In the high voltage regime, Fowler Nordheim tunneling (FNT) is predominant [12]. Here, the I-V relationship is given by

$$I(V) = \mathrm{sgn}(V) \cdot F_1 \cdot S \cdot \frac{e^2 m V^2}{16\pi^2 \hbar m_{\mathrm{o\,x}} \varphi_{\mathrm{B}} t_{\mathrm{B}}^2} \exp\left(-F_2 \cdot \frac{4 t_{\mathrm{B}} \sqrt{2 m_{\mathrm{ox}}} e \varphi_B^{3/2}}{3 + |V|}\right), \quad (4)$$

where $F_1 > 0$ and $F_2 > 0$ are fitting parameters to make the current continuous at the transition voltage from DT to FNT. The equations described above can be used to represent the DC behavior of the FTJ accurately, and have been shown in Fig. 2. The values of φ_1, φ_2 and m are different for the LRS and HRS states, which results in the difference in current in the two states. The values of these parameters are obtained from [13]. The model has been shown to perform reasonably well with FTJ devices made of other ferroelectric materials as well, by substituting the corresponding values of barrier potentials and tunneling mass.

3 Entropy Source

Recall that the change of state in an FTJ occurs via domain nucleation and domain wall propagation [13]. Once a sufficient reverse domain nucleus has been formed, the domain wall propagation takes over domain nucleation. This gives rise to two characteristic stages during the switching process. We consider the Kolmogorov-Avrami-Ishibashi (KAI) model [16] to study the switching characteristics. The ferroelectric film is divided into N independent regions each having its own characteristic nucleation time τ_{Ni}. The percentage of the reversed polarization $s = \frac{\Delta P(t)}{2P_S}$ is written as

$$\frac{\Delta P(t)}{2P_S} = \sum_{i=1}^{N} \lambda_i \times h\left(t - \tau_{Ni}\right) \times \left\{1 - \exp\left[-\left(\frac{t - \tau_{\mathrm{N}i}}{\tau_{\mathrm{P}i}}\right)^2\right]\right\}, \quad (5)$$

where λ_i is the proportion of i-th region to the entire film, $h(t)$ is Heaviside step function, and τ_{Pi} is the characteristic time for domain wall propagation. Note that τ_{Ni} and τ_{Pi} follow Merz's law [17], and are given by

$$\tau_{\mathrm{N,\,P}} = \tau_{\mathrm{0N,0P}} \times \exp\left(\frac{E_{\mathrm{a\,N,\,a\,P}}}{V} t_{\mathrm{B}}\right) = \tau_{\mathrm{0N,0P}} \times \exp\left(\frac{U_{\mathrm{N,\,P}} E_0}{k_{\mathrm{B}} T} \cdot \frac{1}{V} t_B\right), \quad (6)$$

where $E_{\mathrm{aN,aP}}$ is the activation field, $\tau_{0\,\mathrm{N,\,0\,P}}$ is the attempt time, and V is the applied voltage. The values of N and λ_i are stochastic. Also, the characteristic nucleation time (τ_{0Ni}) follows an exponential random distribution. Thus, the time required to switch follows a random variation, which is the basis of the entropy source for *FerroCoin*.

The fraction of reversed polarization is represented by s_{OFF} and can be used as a memristive state variable. When $s_{\mathrm{OFF}} = 1$, all the domains have switched and the device is in HRS. Whereas, $s_{\mathrm{OFF}} = 0$ implies that the device is in LRS. The total current flowing through the FTJ at any intermediate state is given by

$$I = I_{\mathrm{OFF}} \cdot s_{\mathrm{OFF}} + I_{\mathrm{ON}}(1 - s_{\mathrm{OFF}})$$

I_{OFF} and I_{ON} are calculated from $I(V)$ and R_{diff} from eqs. (2-3). The switching characteristics of the FTJ are modeled using s_{OFF}, which is calculated from eqs. (4-6). An analytical solution is developed for the equation and small time steps are assumed in which $s(t)$ remains constant. Then, voltage-dependent $s(t)$ is calculated for each time step, which gives the transient value of I while switching.

It has been reported that the domain nucleation time follows an exponential random distribution [10]. Hence, we model the stochasticity by taking an exponential random distribution of the attempt nucleation time τ_{0Ni}, spread over N regions (which is also stochastic). Here, λ_i is considered to be a constant. The mean attempt to nucleation time is taken as reported in literature [10] for generating the distribution. The switching time is defined as the time taken by the device to change its state from HRS to LRS. This includes both the total nucleation time and the propagation time. A ± 5 V pulse of width 2 ns is applied 100 times. The current variation in the FTJ and the fraction of domains switched is plotted in Fig. 3, which shows clearly the randomness in the switching time. When s_{OFF} reaches 0, the current in the FTJ increases, indicating a change from HRS to LRS.

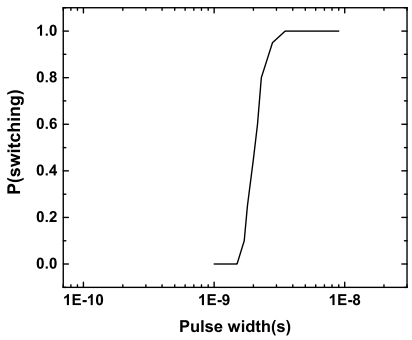


Fig. 4: Probability of switching versus applied pulse width, for the considered FTJ

The probability of switching is plotted against pulse width in Fig. 4. A pulse of the same magnitude and varying pulse width is applied. If the pulse width is less than the switching time, the device does not switch. The point where a 50% probability of switching occurs is chosen as the write time for *FerroCoin*. This implies that applying the selected pulse width across the FTJ multiple times results in switching in half of the cases. When the switching of the domains occur, a higher current is read, as s_{OFF} goes to zero. Conversely, when there is no switching, the domains remain oppositely polarized resulting in a lower current. A sharper switching can therefore cause the current to vary by a large amount within a very short span of time, and thus can be detected easily. Such sharp switching characteristics can be observed in scaled ferroelectric samples with fewer number of domains [10].

4 TRNG Construction and Working

The *FerroCoin* TRNG circuit is constructed from the FTJ as shown in Fig. 5. It consists of the FTJ, biasing circuitry, and peripherals for sampling the bit. The control signals write enable (WE), read enable (RE) and reset enable (ResE) control the switches for each pulse. When a write pulse of magnitude equal to the switching probability of 50% is applied, the device has an equal probability of switching. Thus, when the current is read from the device in the next stage there is an equal probability of it being either in HRS or LRS. This can be sampled using the sampling circuit consisting of a comparator and a latch. A write pulse of magnitude 9.8 V and pulse width of 1.25 ns is applied to the FTJ when WE is on. Thereafter when RE is turned on, a read pulse of magnitude 2 V and width 0.1 ns is applied. The device state is read by measuring the current through the FTJ. A voltage divider arrangement is used to obtain the corresponding voltage. This is sampled using the sampling circuit wherein it is compared with a fixed reference voltage. The reference voltage is chosen such that it is between the high and low voltage states (corresponding to HRS and LRS). This produces an output (V_{out}), which is latched to 1 when (V_{out}) is high, and to 0 when (V_{out}) is low.

The circuit is simulated using *SPECTRE*. For each pulse, a value of $\tau_{0\mathrm{N}}$ and N is selected randomly using a lookup table generated in *MATLAB*. The sampling circuit is designed

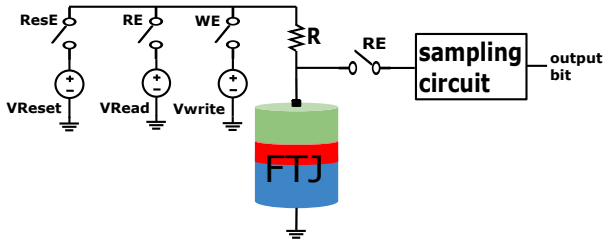


Fig. 5: Circuit diagram of *FerroCoin*, with biasing and sampling peripherals

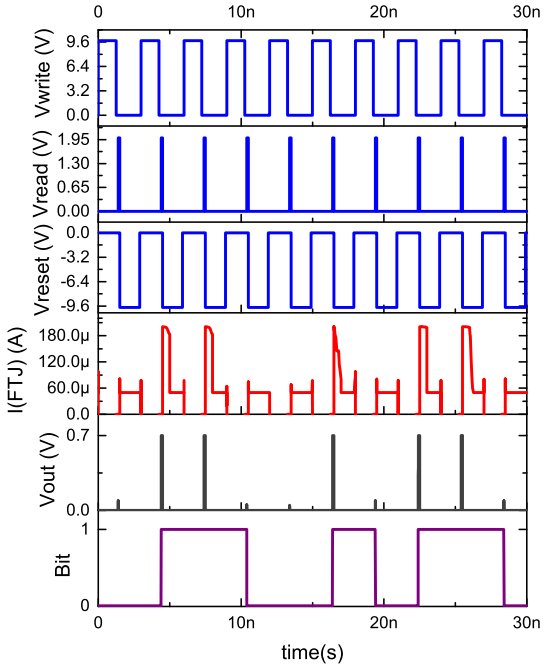


Fig. 6: Timing diagram of *FerroCoin* (10 cycles) showing (i) the write pulse, (ii) the read pulse, (iii) the reset pulse, (iv) the current through the FTJ, (v) the output voltage of the comparator, and (vi) the random bit generated (011010110)

using 22 nm FDSOI, modeled using the industry-standard compact model *BSIM-IMG* [18]. The timing diagram is shown in Fig. 6. The circuit produces a random output bit in every cycle. After the read pulse, a reset pulse of width 1.5 ns is applied. The pulse width of this reset pulse is larger than the write pulse, so that the probability of switching is 1. This is necessary to bring the FTJ to its initial state before the next write pulse is applied.

5 Security Analysis

The *FerroCoin* TRNG circuit presented in section 4 is used to generate random bit streams, 1 million bits in length. The bit streams are then tested using the NIST 800-22 statistical test suite [19], which consists of 15 standardized tests to evaluate the randomness of the entropy source. The tests return a figure of merit known as the p-value, and a p-value greater than 0.01 implies that the input bit stream is statistically random with 99 percent confidence levels. Further details about the individual tests can be found in [19]. We generate

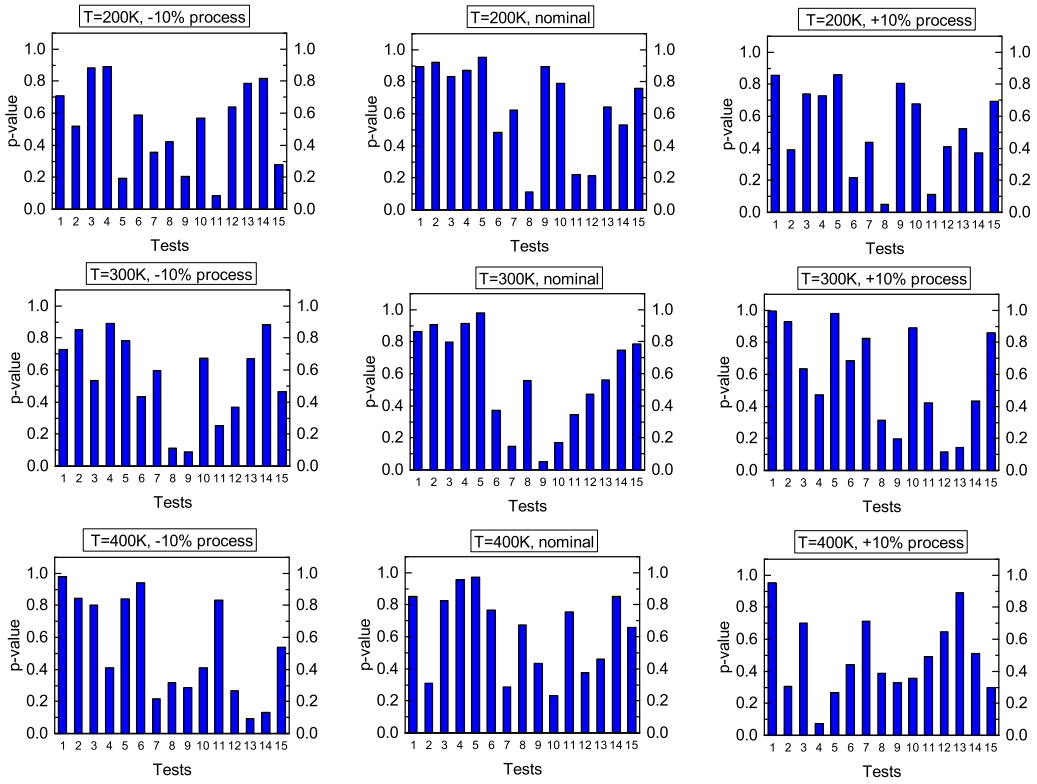


Fig. 7: Average p-values from the NIST 800-22 statistical test suite for various process and temperature corners. The tests in order are: (1) Approximate Entropy Test, (2) Block Frequency Test, (3) Cumulative Sums (Forward) Test, (4) Fast Fourier Transform Test, (5) Frequency Test, (6) Linear Complexity Test, (7) Longest Run of Ones Test, (8) Non-overlapping Templates test, (9) Overlapping Templates Test, (10) Rank Test, (11) Runs Test, (12) Random Excursions Test, (13) Random Excursions (Variant) Test, (14) Serial Test, and (15) Universal Test.

10 bit streams each for nine process and temperature corners (T = 200 K, 300 K, 400 K; process = -10%, 0%, +10%). We observe that 10/10 sequences pass all the NIST 800-22 tests, for all the corners considered. This confirms that the ferroelectric domain switching phenomenon is indeed a promising source of entropy for TRNG implementations. Note that the process variation of $\pm$10% is considered in the thickness of ferroelectric layer. The average p-values across the 10 bit streams, for each process and temperature corner, are highlighted in Fig. 7.

6 *FerroCoin* Benchmarking

The performance and on-chip implementation feasibility of a TRNG can be evaluated using some important quantitative metrics such as the power, bit rate, and the energy consumed per bit.

6.1 Performance Evaluation

Here, we obtain the power and energy/bit directly from the *SPECTRE* simulations by calculating the average power consumed and the energy required to generate a single bit in one cycle. The total period, which includes the write, read and reset pulses for one cycle, gives us a measure of the bits generated per second or the bit rate. The area is obtained using post-synthesis layout based on 22 nm *PTM* models [20]. The performance metrics of *FerroCoin*, implemented using Co/BTO/LSMO stack, are shown in Table 1 for three different temperatures.[1]

TABLE 1: Performance metrics of *FerroCoin*

Temperature	Bit Rate (Mbps)	Power (μW)	Energy/bit (pJ)	Area (μm^2)
200 K	277	29.44	0.106	
300 K	333	36.29	0.109	4.085
400 K	357	39.55	0.110	

The bit rate of *FerroCoin* is comparable to state-of-the-art TRNGs. At higher temperatures, the energy barrier is lower and thus the nucleation time is reduced, although the difference is not much. The switching is more frequent at higher temperatures, which draws a higher power. The summarized results show that the proposed *FerroCoin* TRNG is highly robust to external temperature variations.

6.2 Material Optimization

In order to further improve the bit rate and lower power consumption, we perform material-level analysis and optimization. In this regard, we choose three other suitable FTJ material stacks, namely (i) Ag/$BaTiO_3$(BTO)/Nb:$SrTiO_3$(NSTO) [21],

1. The performance metrics, i.e - power and bit rate are calculated from pre-synthesis simulations without considering the parasitic resistance and capacitance. Including the effect of parasitics at every node increases the power by $\sim$8 % and reduces the bit-rate by $\sim$14 %.

(ii) $TiN/HfZrO_2(HZO)/Al_2O_3/TiN$ [22], and (iii) $Co/PbZrTiO_3(PZT)/LSMO$ [23].

TABLE 2: Parameters for the different FTJ material stacks

Material Stack	V_{sw} (V)	τ (ns)	T_{fe} (nm)	I_{on} (μA)	I_{off} (μA)
Co/BTO/LSMO [13]	9.6	1.8	2	6.1	0.095
Ag/BTO/NSTO [21]	10	0.8	2.4	4.9	0.01
$TiN/HZO/Al_2O_3/TiN$ [22]	6.5	100	12	0.003	0.0002
Co/PZT/LSMO [23]	8	6	1.6	0.017	0.002

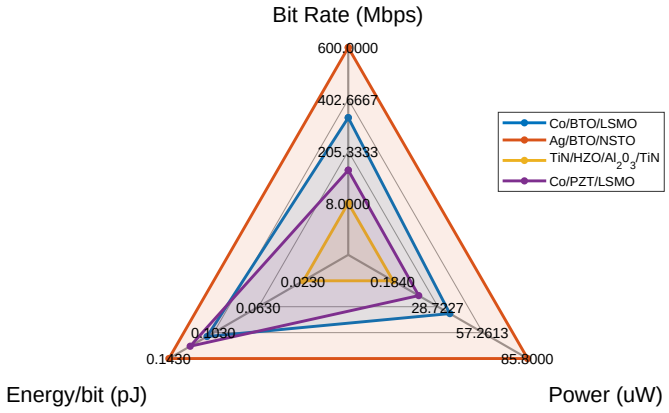


Fig. 8: Comparison of performance metrics of *FerroCoin* with different FTJ material stacks

TABLE 3: Comparison with state-of-the-art TRNGs

TRNG	Power (μW)	Bit Rate (Mbps)	Area (μm^2)
MTJ-based (45 nm) [3]	136.3	244	12.07
ReRAM-based [4]	1280	32	2.56
2D material-based [6]	1000	0.001	NA
Neuromorphic spintronic structure-based (10 nm) [7]	55.37	50	1.05 (219 UST)
FerroCoin (22 nm)	**36.297**	**333**	**4.085**

The parameters of the materials such as φ and mean value of τ_N are adjusted so as to achieve proper I-V characteristics and switching as reported in the literature (See Table 2.) Then, the TRNG circuit is simulated using these FTJ stacks. The comparison of the performance metrics for the different FTJ material stacks is shown in Fig. 8. It is seen that HfO_2-based FTJ has a lower bit rate due to reduced switching time. However, it also has a lower power consumption due to low current and switching voltage. PZT-based materials have been demonstrated to show sub-ns switching. This allows TRNG based on these FTJs to have a high bit rate, at the cost of increased power. Thus, our material-level analysis clearly shows a trade-off between the consumed power and the bit rate. Hence, one should carefully examine the application for which the TRNG is to be deployed and choose the FTJ material stack accordingly. If the TRNG is to act as a seed for a Pseudo Random Number Generator, which can generate random numbers at Gbits/second from a single seed, then we might get away with a lower bit rate and thus achieve high power efficiency. However, if the TRNG is to be directly used for generating random numbers for encryption or in hardware security modules, then we require a higher bit rate at the cost of increased power consumption, which can be achieved with PZT materials. Thus, the *FerroCoin* TRNG implementation offers huge versatility and optimization, to tailor the FTJ material stack according to the requirements of the application.

6.3 Comparison with Prior Art

Table 3 shows the comparison of *FerroCoin* with prior art. Note that the comparison is shown for *FerroCoin* using Co/BTO/LSMO as the FTJ stack. The proposed *FerroCoin* circuit not only offers a higher bit rate but also consumes much lower power as compared to other TRNGs. This paves way for a new era of stochastic computing using ferroelectric materials, which provides all the necessary performance benefits of a TRNG, without any post processing and at a very low power. The comparatively higher area for our proposed TRNG can be reduced further by using advanced FinFET-based technological nodes for the peripheral design.

6.4 Challenges and Future Work

A major challenge for *FerroCoin* arises from the limited cycling endurance of ferroelectric materials, especially HZO. To alleviate this reliability issue, a memory crossbar array architecture can be used. The presence of redundant FTJs in the crossbar array effectively reduces the number of times each FTJ has to be switched. Further, manufacturing defect-induced biases in highly scaled FTJ processes can also be countered by using a crossbar array implementation. Our proposed design is perfectly suited for crossbar implementation as only a single comparator can be used for all the cells in a given row/column. Another challenge for *FerroCoin* stems from the difficulty of integrating perovskite-based ferroelectric materials into modern foundry processes. This can restrict the high-bit rate applications for our on-chip TRNG, as these perovskite-based ferroelectrics typically showcase high switching speeds. Recently however, HZO-based materials have also been reported with high switching speeds and endurance [24], [25]. Thus, an HZO-based *FerroCoin* could possibly address the problem of fabrication maturity, while also providing high bit rates and endurance.

7 Conclusion

There is a need for a robust, reliable and low power TRNG, requiring minimal post-processing, in the cryptography, hardware security, and general integrated circuit application space. In this paper, we address this need by proposing *FerroCoin*, a TRNG leveraging the entropy in the ferroelectric domain switching phenomenon of FTJs. *FerroCoin* is shown to exhibit competitive power, bit rate and energy/bit metrics compared to prior state-of-the-art, and also passes the NIST 800-22 statistical test suite for randomness. Further, the material optimizations and trade-offs presented for *FerroCoin* in this paper showcase its versatility and potential for on-chip implementation.

REFERENCES

[1] S. M. and K. Ç.K., "True Random Number Generators," in *Open Problems in Mathematics and Computational Science. Springer, Cham.* [Online]. Available: https://doi.org/10.1007/978-3-319-10683-0_12

[2] E. Kim, M. Lee, and J.-J. Kim, "8Mb/s 28Mb/mJ robust true-random-number generator in 65nm CMOS based on differential ring oscillator with feedback resistors," in *2017 IEEE International Solid-State Circuits Conference (ISSCC)*, 2017, pp. 144–145.

[3] N. Rangarajan, A. Parthasarathy, and S. Rakheja, "A spin-based true random number generator exploiting the stochastic precessional switching of nanomagnets," *Journal of Applied Physics*, vol. 121, no. 22, p. 223905, 2017.

[4] Z. Wei, Y. Katoh, S. Ogasahara, Y. Yoshimoto, K. Kawai, Y. Ikeda *et al.*, "True random number generator using current difference based on a fractional stochastic model in 40-nm embedded ReRAM," in *2016 IEEE International Electron Devices Meeting (IEDM)*, 2016, pp. 4.8.1–4.8.4.

[5] B. Ray and A. Milenkovic, "True Random Number Generation Using Read Noise of Flash Memory Cells," *IEEE Transactions on Electron Devices*, vol. PP, pp. 1–7, 02 2018.

[6] A. Wali, H. Ravichandran, and S. Das, "A Machine Learning Attack Resilient True Random Number Generator Based on Stochastic Programming of Atomically Thin Transistors," *ACS Nano*, Oct 2021. [Online]. Available: https://doi.org/10.1021/acsnano.1c05984

[7] A. Amirany, K. Jafari, and M. H. Moaiyeri, "True Random Number Generator for Reliable Hardware Security Modules Based on a Neuromorphic Variation-Tolerant Spintronic Structure," *IEEE Transactions on Nanotechnology*, vol. 19, p. 784–791, Jan. 2020.

[8] Y. Wang, W. Wen, H. Li, and M. Hu, "A Novel True Random Number Generator Design Leveraging Emerging Memristor Technology," in *Proceedings of the 25th Edition on Great Lakes Symposium on VLSI*, ser. GLSVLSI '15. New York, NY, USA: Association for Computing Machinery, 2015, p. 271–276.

[9] H. Mulaosmanovic, T. Mikolajick, and S. Slesazeck, "Random number generation based on ferroelectric switching," *IEEE Electron Device Letters*, vol. 39, no. 1, pp. 135–138, 2018.

[10] H. Mulaosmanovic, J. Ocker, S. Müller, U. Schroeder, J. Müller, P. Polakowski *et al.*, "Switching Kinetics in Nanoscale Hafnium Oxide Based Ferroelectric Field-Effect Transistors," *ACS Applied Materials & Interfaces*, vol. 9, no. 4, pp. 3792–3798, Feb 2017.

[11] A. M. Ionescu, "Ferroelectric devices show potential," *Nature Nanotechnology*, vol. 7, no. 2, pp. 83–85, Feb 2012.

[12] D. Pantel and M. Alexe, "Electroresistance effects in ferroelectric tunnel barriers," *Phys. Rev. B*, vol. 82, p. 134105, Oct 2010.

[13] Z. Wang, W. Zhao, W. Kang, A. Bouchenak-Khelladi, Y. Zhang, Y. Zhang *et al.*, "A physics-based compact model of ferroelectric tunnel junction for memory and logic design," *Journal of Physics D:Applied physics*, vol. 47, no. 4, p. 045001, Dec. 2013.

[14] W. F. Brinkman, R. C. Dynes, and J. M. Rowell, "Tunneling Conductance of Asymmetrical Barriers," *Journal of Applied Physics*, vol. 41, no. 5, pp. 1915–1921, 1970.

[15] A. Gruverman, D. Wu, H. Lu, Y. Wang, C. Jang, H.W.and Folkman, M. Zhuravlev *et al.*, "Tunneling electroresistance effect in ferroelectric tunnel junctions at the nanoscale," *Nano letters*, vol. 9, no. 10, pp. 3539–3543, 2009.

[16] Y. Ishibashi and Y. Takagi, "Note on Ferroelectric Domain Switching," *Journal of the Physical Society of Japan*, vol. 31, no. 2, pp. 506–510, 1971.

[17] W. J. Merz, "Domain Formation and Domain Wall Motions in Ferroelectric $BaTiO_3$ Single Crystals," *Phys. Rev.*, vol. 95, pp. 690–698, Aug 1954.

[18] P. Kushwaha, H. Agarwal, S. Khandelwal, J.-P. Duarte, A. Medury, C. Hu *et al.*, "BSIM-IMG: Compact model for RF-SOI MOSFETs," in *2015 73rd Annual Device Research Conference (DRC)*, 2015, pp. 287–288.

[19] L. Bassham, A. Rukhin, J. Soto, J. Nechvatal, M. Smid, S. Leigh *et al.*, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic applications," 2010-09-16 2010. [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762

[20] Nanoscale Integration and Modeling (NIMO) Group at ASU. Predictive Technology Models. [Online]. Available: http://ptm.asu.edu/

[21] C. Ma, Z. Luo, W. Huang, L. Zhao, Q. Chen, Y. Lin *et al.*, "Sub-nanosecond memristor based on ferroelectric tunnel junction," *Nature Communications*, vol. 11, no. 1, p. 1439, Mar 2020.

[22] B. Max, M. Hoffmann, S. Slesazeck, and T. Mikolajick, "Direct Correlation of Ferroelectric Properties and Memory Characteristics in Ferroelectric Tunnel Junctions," *IEEE Journal of the Electron Devices Society*, vol. 7, pp. 1175–1181, 2019.

[23] D. Pantel, H. Lu, S. Goetze, P. Werner, D. Jik Kim, A. Gruverman *et al.*, "Tunnel electroresistance in junctions with ultrathin ferroelectric $Pb(Zr_{0.2}Ti_{0.8})O_3$ barriers," *Applied Physics Letters*, vol. 100, no. 23, p. 232902, 2012.

[24] T. Mikolajick, S. Slesazeck, H. Mulaosmanovic, M. H. Park, S. Fichtner, P. D. Lomenzo *et al.*, "Next generation ferroelectric materials for semiconductor process integration and their applications," *Journal of Applied Physics*, vol. 129, no. 10, p. 100901, 2021. [Online]. Available: https://doi.org/10.1063/5.0037617

[25] X. Lyu, M. Si, P. R. Shrestha, K. P. Cheung, and P. D. Ye, "First direct measurement of sub-nanosecond polarization switching in ferroelectric hafnium zirconium oxide," in *2019 IEEE International Electron Devices Meeting (IEDM)*, 2019, pp. 15.2.1–15.2.4.