Proposal for True Random Number Generation in ferroelectric capacitors using noise-induced switching

Madhav Ramesh[1], Amit Verma[2], and Arvind Ajoy[3]

[1]Cornell University, [2]Indian Institute of Technology Kanpur, [3]Indian Institute of Technology Palakkad

Abstract

A true random number generator that leverages the energetic bistability of the polarisation in a ferroelectric capacitor is proposed. Our theoretical analysis and numerical simulation results show that the addition of thermal noise and an appropriately chosen voltage pulse to this device facilitates tunable, but probabilistic switching between two stable polarisation states.

Keywords: True random number generators (TRNG), Kramers' escape problem, ferroelectrics

Introduction

Random number generation finds numerous applications ranging from cryptography to numerical simulations [1]. A key component of these systems are hardware-based true random number generators (TRNG) [2], which utilize an inherent source of entropy as opposed to pseudo random number generators (PRNGs) which are algorithm-based. Defect mechanisms in materials can be exploited as entropy sources. For example, Mulaosmanovic et al. used the domain wall motion induced polarisation fluctuations (a Poisson process) in ferroelectric HfO$_2$ based field-effect transistor to demonstrate a TRNG [3]. Other TRNGs have also recently been developed using ferroelectric random access memory (FRAM) technology [4]. In this work, we propose the utilization of thermal noise in ferroelectric materials, which provides a "tunable" source of randomness as opposed to the above approaches.

A ferroelectric capacitor demonstrates hysteresis in its polarisation-voltage characteristics. Application of a voltage pulse with magnitude greater than the coercive voltage V_c causes deterministic polarisation switching due to the disappearance of the barrier separating the two stable states (see Fig. 1(c)). However, stochastic switching (SS) can happen for voltages less than V_c when aided by noise (see Fig. 1(d)) – this process is often referred to as stochastic resonance [5]. Our proposal seeks to utilize SS for TRNG applications.

We note here that the dynamics of SS due to noise is similar to the classical Kramers' escape problem, which deals with the dynamics of the escape of a strongly damped Brownian particle from a potential well, over an energy barrier [6]. The basic theory is outlined in the next section, wherein we map the Landau-Ginzburg-Devonshire (LGD) theory of polarisation dynamics of a homogeneous ferroelectric with Kramers' escape problem. Based on this, we propose a voltage pulsing scheme for using a ferroelectric capacitor as a TRNG. We check our analytical results using numerical solution of the relevant stochastic differential equations. Lastly, we show some preliminary results from the NIST statistical test suite [7] to test generated bit randomness.

Theory

The free energy density F (in J/m^3) of a homogeneous ferroelectric with polarisation P is given by [8]

$$F = \alpha P^2 + \beta P^4 - PE, \tag{1}$$

where E is the electric field and α and β are the Landau coefficients. Then, the time-dependent LGD equation is

$$\rho \frac{\partial P}{\partial t} = -\frac{\partial F}{\partial P} + \xi(t), \tag{2}$$

where $\xi(t)$ is the noise and ρ is the resistivity of the ferroelectric. Note that eq. (2) resembles the Langevin equation for dynamics of a Brownian particle when displacement is mapped to polarisation. $\xi(t)$ can arise from internal fluctuations in the ferroelectric, apart from the external noise voltage with r.m.s. value V_{noise}. Assuming that both these contributions are Gaussian white noise, the auto-correlation is

$$\langle \xi(t)\xi(t') \rangle = 2(D_{int} + D_{ext}) \cdot \rho \cdot \delta(t - t') \tag{3}$$

$$\text{with } D_{int} = \frac{k_B T}{t_F A_F} \tag{4}$$

$$\text{and } D_{ext} = \frac{V_{noise}^2}{2R_F} \frac{1}{\Delta f} \frac{1}{t_F A_F} \tag{5}$$

from the Fluctuation-Dissipation relation, which relates the fluctuating and dissipative forces in the system. Here, k_B is Boltzmann's constant and T is the temperature of the system. t_F and A_F represent the thickness and area respectively of the ferroelectric. Δf represents the bandwidth of the noise.

Then, with analogy from the classical Kramers' problem [9], [10], the rate of escape of the state of polarisation over the energy barrier (Kramers rate) r_K where

$$r_K = \frac{1}{t_K} = \frac{\sqrt{|F''(P_A)F''(P_C)|}}{2\pi\rho} \exp\left(-\frac{\Delta F}{D_{ext}}\right) \tag{6}$$

Readers may refer to Figure 2(a) for the notations. The reciprocal of r_K is t_K, which is referred to as Kramers time. This particular metric can be interpreted as the average time spent in the well around point A, before a

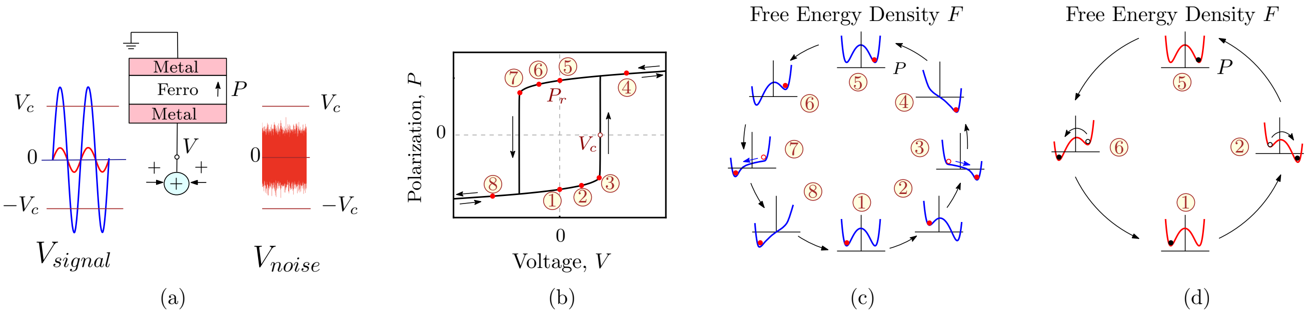

Fig. 1. Ferroelectric capacitor (a) demonstrating deterministic switching (b,c) when $V_{signal} > V_c, V_{noise} = 0$ with disappearance of the barrier and (d) stochastic switching when $V_{signal} < V_c$ aided with appropriate V_{noise}.

transition is made over point C at the top of the barrier. Note that the ratio $D_{ext}/\Delta F$ ($D_{ext} \gg D_{int}$) provides a scale for the noise, since it determines Kramers time.

Simulations and TRNG Methodology

In this work, we consider Hafnium Zirconium Oxide ($Hf_{1\text{-}x}Zr_xO_2$ or HZO) as the ferroelectric. All relevant parameters have been listed in Table I.

$$\alpha = \frac{-3\sqrt{3}E_c}{4P_r} \text{ and } \beta = \frac{3\sqrt{3}E_c}{8P_r^3} \tag{7}$$

We solve eq. (2) using the Euler-Maruyama method [11]. In discrete form, with $D_{ext} \gg D_{int}$, we have

$$P[i] = P[i-1] - \frac{\Delta t}{\rho} \cdot \frac{dF}{dP}[i] + \sqrt{\frac{2D_{ext}}{\rho}} \cdot \Delta W[i] \tag{8}$$

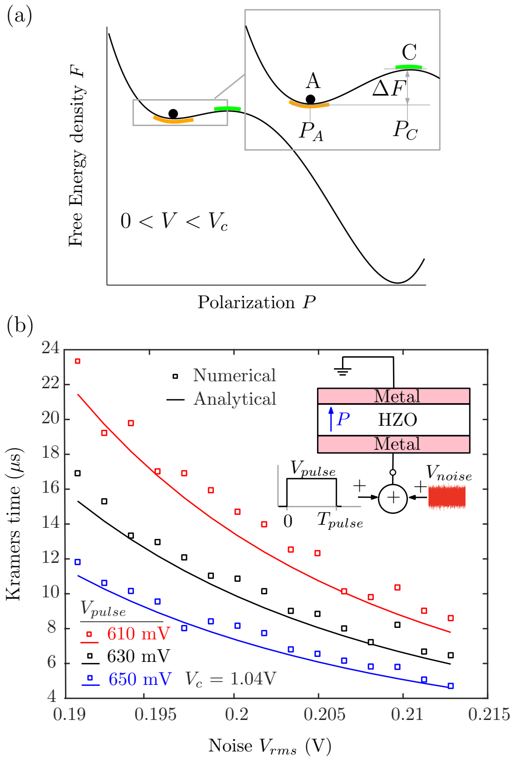

Fig. 2. (a) Kramers' escape problem applied to the polarisation state in a ferroelectric. (b) Verification of Kramers time. Our simulation results match the analytical predictions, based on eq. (6), very well.

TABLE I: Parameters of HZO capacitors [12]

Parameter	Value
Thickness t_F (nm)	10
α (mF^{-1})	-7.603×10^8
β ($m^5F^{-1}C^{-2}$)	1.204×10^{10}
Remnant Polarisation P_r ($\mu C/cm^2$)	17.76
Coercive Field E_c (MV/cm)	1.04
Coercive Voltage V_c (V)	1.04
Resistivity ρ ($\Omega - m$)	30
Temperature T (K)	300
Area A_F (μm^2)	1

where $[i]$ represents the i^{th} time-step. The term $\Delta W[i]$ is obtained by extracting numbers from a normal distribution with mean 0 and variance Δt. For our simulations, we selected a time step $\Delta t = 1$ ns.

Figure 2(b) presents the results of our simulations for Kramers time t_K, compared with the analytical results predicted by eq. (6). The polarisation is initially assumed to be in the left well. A positive voltage pulse with amplitude V_{pulse} is applied such that the double well is asymmetric. A significantly large pulse width $T_{pulse} = 90\mu s$ has been taken (about 4× larger than the highest value of Kramers time) such that a switching event is almost certainly guaranteed. An ensemble of 300 systems have been considered (for each V_{noise} and V_{pulse}), with the average time spent in the well before a switching event occurring being recorded. This solver is used to investigate the TRNG application.

We can define a switching probability, $S(t)$, as the probability of a particle switching from one well to the other over time [9]. Based on our analogy, instead of a particle in a well, we track the polarisation state of the ferroelectric.

$$S(t) = 1 - e^{-r_K t} \tag{9}$$

See Fig. 3. To initialise to a '0', a negative reset pulse value below the coercive voltage $-V_c$ is applied. Subsequently, the optimal voltage value V_{switch} and pulse width T_{pulse} can be selected based on eq. (9). For a given noise intensity and voltage pulse height, there is a corresponding r_K. Therefore, it is possible to

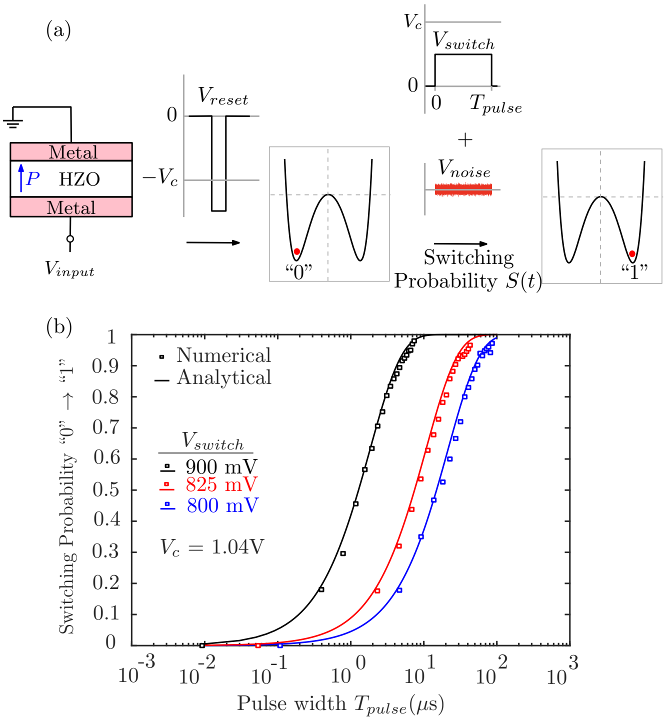

Fig. 3. (a) Schematic showing the use of external noise with a ferroelectric to generate random numbers. A reset pulse sets the system in the "0" state. Subsequently, a voltage pulse (with amplitude V_{switch} and width T_{pulse}) and external noise V_{noise} causes the system to switch from "0" → "1". (b) Switching probability for different input voltages in HZO. Noise is fixed, with $V_{rms} = 126$mV and a bandwidth of 10MHz.

achieve any probability value for '0' or '1' by varying the pulse width. By integrating the ferroelectric into a device like a transistor, one may realise a TRNG with tunability. The thermal noise may be given from an external resistor [13]. This introduces an element of tunability aside from the voltage pulse height and width.

By taking multiple input noise voltages and pulse widths, it is possible to obtain numerical fits for eq. (9). For each of these values, the probability has been found by computing the number of switching events for an ensemble (of size 500 in this work) and dividing by the total number of members of this ensemble. This result is shown in Fig. 3. The numerical results match the analytical predictions (eq. (9)) very well. For a TRNG, $S(t) \approx 50\%$, for which $T_{pulse} \approx t_K \ln 2$.

As a step to test randomness, one hundred 1000 bit sequences were put through the first five NIST tests [7]. For $V_{switch} = 800$mV, $V_{rms} = 126$mV and $T_{pulse} = 16\mu$s ($S(t) = 52\%$), a pass rate of 98/100 sequences and higher was obtained, which is greater than the requirement of 96/100 to be classified as random. These results are promising, and further optimisation can result in more reliable TRNGs.

Conclusion

We presented simulation results for true random number generation in a ferroelectric (HZO), under the assumption of homogeneous switching. In addition, we provided the theoretical foundation for a potential ferroelectric device application based on Kramers' escape problem. Our results suggest that it is possible to add an element of tunability to the inherent randomness in the system through the bistable nature of ferroelectrics. Moreover, preliminary tests for randomness show a high pass rate. This could potentially lead to new devices that would lead to advances in data security.

Acknowledgment

The authors gratefully acknowledge the use of the CHANDRA High Performance Computing cluster at IIT Palakkad. AA thanks SERB (Science and Engineering Research Board, Government of India) for support through MTR/2021/000823 and CRG/2022/008128. AV thanks SERB Early Career Research Award (Grant No. ECR/2018/001076) for supporting the SURGE internship of MR.

References

[1] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Rev Mod Phys*, vol. 89, no. 1, p. 015004, 2017.

[2] L. Gong, J. Zhang, H. Liu, L. Sang, and Y. Wang, "True random number generators using electrical noise," *IEEE Access*, vol. 7, pp. 125 796–125 805, Sep. 2019.

[3] H. Mulaosmanovic, T. Mikolajick, and S. Slesazeck, "Random number generation based on ferroelectric switching," *IEEE Electron Device Lett.*, vol. 39, no. 1, pp. 135–138, Nov. 2017.

[4] E. T. Peeters, W. F. Kraus, M. G. Aguilar, and J. A. Rodriguez, "Random number generation with ferroelectric random access memory," Feb. 26 2019, US Patent 10,216,484.

[5] C. Drozhdin, "Stochastic Resonance in Ferroelectric TGS Crystals," Ph.D. dissertation, Martin-Luther-University Halle-Wittenberg, Nov. 2001.

[6] H. A. Kramers, "Brownian motion in a field of force and the diffusion model of chemical reactions," *Physica*, vol. 7, no. 4, pp. 284–304, Apr. 1940.

[7] A. Rukhin, J. Soto *et al.*, *A statistical test suite for random and pseudorandom number generators for cryptographic applications.* US DOC, TA, NIST, 2001, vol. 22.

[8] S. Etesami, A. Sukhov, and J. Berakdar, "Kinetics of nanosize ferroelectrics," *Phys. Rev. B*, vol. 94, no. 17, p. 174105, 2016.

[9] R. Metzler and J. Klafter, "Kramers' escape problem with anomalous kinetics: non-exponential decay of the survival probability," *Chem. Phys. Lett.*, vol. 321, pp. 238–242, 2000.

[10] M. Ramesh, A. Verma, and A. Ajoy, "Kramers' escape problem for white noise driven switching in ferroelectrics," *arXiv preprint arXiv:2112.01373*, 2021.

[11] E. Platen, "An introduction to numerical methods for stochastic differential equations," *Acta numer.*, vol. 8, pp. 197–246, 1999.

[12] M. Si, C.-J. Su, C. Jiang, N. J. Conrad, H. Zhou *et al.*, "Steep-slope hysteresis-free negative capacitance MoS_2 transistors," *Nat. Nanotechnol.*, vol. 13, no. 1, pp. 24–28, Jan. 2018.

[13] C. S. Petrie and J. A. Connelly, "A noise-based ic random number generator for applications in cryptography," *IEEE TCAS-I*, vol. 47, no. 5, pp. 615–621, 2000.