Random Number Generation Based on Ferroelectric Switching

Halid Mulaosmanovic, Thomas Mikolajick, *Senior Member, IEEE*, and Stefan Slesazeck

***Abstract*— Hafnium oxide-based ferroelectric field-effect transistors (FeFETs) have a great potential for fast non-volatile memory due to their high performance, fully CMOS compatible integration, and low-power operation. The aggressive scaling of these devices has revealed novel features, such as the multilevel storage capability and abrupt switching, which, however, appears to be a stochastic process. In this letter, we propose a path for true random number generation based on the statistical switching in a single FeFET device. It relies on an inherent randomness of the polarization reversal of ferroelectric domains in the gate stack. The bit sequence is generated by repeatedly programming an FeFET at a calibrated voltage and pulse width, and features random and equiprobable "ones" and "zeros," which are separated by orders of magnitude in drain current. This simple yet reliable operation provides a compact one-transistor solution for the unbiased random number generation.**

***Index Terms*— Cryptography, ferroelectric FET (FeFET), ferroelectric memory, random number generation (RNG).**

I. Introduction

SECURE encryption in transmission protocols relies on the random number generators (RNGs). The highest level of security is only ensured when true RNGs are adopted [1]. This is due to the fact that, unlike pseudo-RNGs, a true RNG harnesses an inherent randomness of a certain physical phenomenon and is therefore externally unpredictable and irreproducible.

Many concepts of true RNGs utilizing conventional CMOS circuits have been proposed, exploiting e.g. the random telegraph noise (RTN) in MOSFETs [2], the thermal noise in combination with a jittered oscillator sampling [3], [4], the time to oxide breakdown under voltage stress [5] etc. However, these techniques require a large circuitry for the processing of the random signal and more compact solutions are therefore preferred. With the advent of emerging nonvolatile memory devices, intrinsic stochastic phenomena normally occurring in device operation were described as promising entropy sources for true RNGs. For instance, the variability in resistive random access memory (RRAM), which represents one of its major weaknesses, is exploited to produce randomness. In fact, random fluctuation of resistance upon RTN [6] or variability of the main parameters (set/reset voltage, resistance in the low and high resistive state) [7] in RRAM devices can be readily used for this purpose. Similarly, the stochastic nature of spin-torque switching in a magnetic tunnel junction (MTJ) [8], [9] has been proposed for RNGs as well.

Among novel nonvolatile memory concepts, ferroelectric field-effect transistors (FeFETs) have recently emerged as promising candidates due to their high performance, fully CMOS compatible integration and low-power operation [10], [11]. The aggressive thickness and lateral scaling down to the size of single ferroelectric domains have, however, brought to light novel phenomena such as abrupt and stochastic switching [12]. Such a feature has already opened a path for a potential multi-level storage [13]. In this work, we propose a true RNG based on the switching variability in a single ultra-scaled FeFET device. The clear advantage of this concept lies in its simple 1–transistor (1T) structure, allowing for a compact and highly scalable on-chip true RNG.

II. Experimental Results

A. Stochastic Switching

Our FeFET devices comprise a polysilicon – TiN (8 nm) – HfO_2 (10 nm) – SiON (1.2 nm) gate stack and are fabricated using the 28 nm high-k metal gate process flow in a conventional gate first approach, as described in [10]. The ferroelectric phase in HfO_2 is promoted by a 4 mol% Silicon doping. The channel length and width are 30 nm and 80 nm, respectively.

The channel conductivity of a FeFET can be tuned by switching the polarization charge within the ferroelectric. In fact, by applying a positive gate pulse ($V_G = V_P$) while grounding all other terminals, the polarization is aligned downward and the device is set into a low-V_T state (red curve in Fig. 1a, program operation), where V_T is the threshold voltage. A proper negative V_N pulse, instead, resets the device into the high-V_T state (blue curve in Fig. 1(a), erase operation). The two states are separated by orders of magnitude,

Manuscript received October 16, 2017; revised November 5, 2017; accepted November 6, 2017. Date of publication November 9, 2017; date of current version December 27, 2017. This work was supported by the Free State of Saxony, Germany. The review of this letter was arranged by Editor B. S. Doyle. *(Corresponding author: Halid Mulaosmanovic.)*

H. Mulaosmanovic and S. Slesazeck are with NaMLab gGmbH, 01187 Dresden, Germany (e-mail: halid.mulaosmanovic@namlab.com).

T. Mikolajick is with NaMLab gGmbH, 01187 Dresden, Germany, and also with the Chair of Nanoelectronic Materials, TU Dresden, 01062 Dresden, Germany.

Color versions of one or more of the figures in this letter are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/LED.2017.2771818

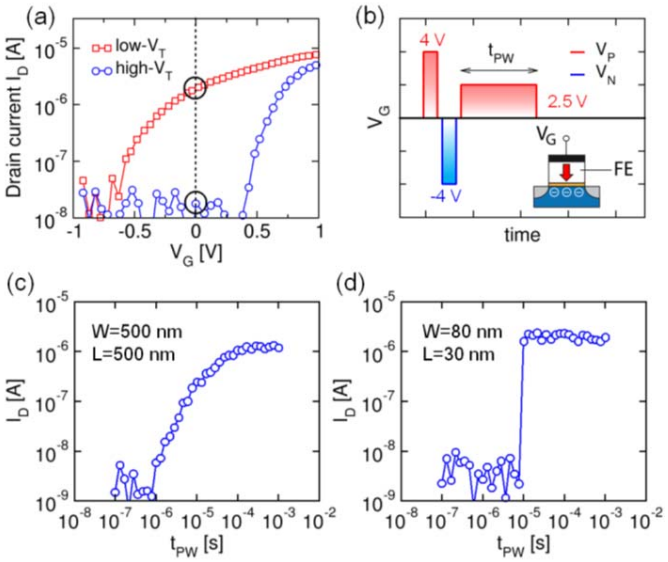

Fig. 1. (a) Transfer curves for the programmed (after gate pulse $V_G = V_P > 0$, red curve) and erased (after gate pulse $V_G = V_N < 0$, blue curve) state of a FeFET having $L = 30$ nm and $W = 80$ nm. The curves are measured at drain voltage $V_D = 100$ mV by a fast V_G sweep, which limits the lower resolution to 10 nA. The two states can be distinguished as a drain current (I_D) level at $V_G = 0$ V along the vertical dashed line. (b) V_G pulse sequence adopted to study the switching from high- to low-V_T state consists of 1) initialization program pulse ($V_P = 4$ V, 1 μs); 2) erase pulse ($V_N = -4$ V, 1 μs) to set the reference high-V_T state; and 3) program pulse $V_P = 2.5$ V with variable pulse width t_{PW}, which explores the time dependent switching. Inset: schematic illustration of a FeFET, where the ferroelectric layer is indicated with FE; Size dependent switching: drain current as a function of t_{PW} for (c) a large area FeFET ($W = L = 500$ nm) and (d) a scaled FeFET ($W = 80$ nm, $L = 30$ nm).

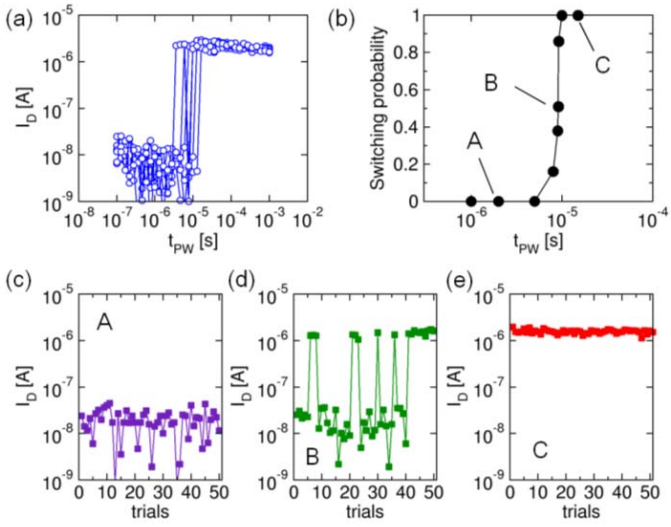

Fig. 2. (a) Stochastic switching around $t_{PW} = 10$ μs of a scaled FeFET for six repetitions of the waveform in Fig. 1(b) with identical set of parameters. (b) Probability switching curve resulting from 50 repetitions of the sequence of Fig. 1(b) for different t_{PW} swept in the proximity of the nominal switching pulse width of 10 μs. The curve presents three distinct regions A, B, and C. A is characterized by no switching (c); in B probabilistic switching takes place (d); and in C deterministic switching can be observed (e).

when the drain current I_D levels are sensed at a proper gate voltage ($V_G = 0$ V is chosen in Fig. 1(a) and throughout this letter). This feature may be exploited to store the binary information in a nonvolatile manner [10], [11].

The switching behavior from one state to the other depends, however, on the device size. It is well known that FeFETs having relaxed lateral dimensions (e.g. $W = L = 500$ nm) show a gradual switching upon a gate excitation with progressively increasing pulse width (Fig. 1(b)) [14], [15], as shown in Fig. 1(c). In contrast, our recent report [12] on the aggressively scaled devices has revealed an additional switching feature. Indeed, when the channel length is comparable to the ferroelectric domain size and hence the gate stack contains only one or a few switchable domains, the switching becomes extremely sharp, as exemplarily shown in Fig. 1(d) for the transition from high- to low-V_T state.

Moreover, it was shown that this switching is a stochastic rather than a deterministic process, when the device is excited in the proximity of the ferroelectric coercive voltage. The phenomenon can be easily captured in an experiment where the V_G waveform of Fig. 1(b) is repeated several times on the same device: even if the entire set of experimental parameters (V_N, V_P and t_{PW}) is completely identical, the pulse width at which the abrupt switching occurs shows a certain spread around a nominal value of $t_{PW} = 10$ μs for $V_P = 2.5$ V, as shown in Fig. 2(a). This means the exact switching time is *a priori* unpredictable. Such a stochastic behavior is attributed to the intrinsic switching variability coming from the nucleation driven polarization reversal in the ferroelectric and can be modeled with a Poisson process in the time domain [12].

This can be further appreciated in Figures 2(b)-2(e): Fig. 2(b) shows the probability of a high- to low-V_T switching resulting from 50 repetitions of the sequence of Fig. 1(b) for different t_{PW}, which are finely swept in the proximity of the nominal switching time 10 μs. The curve is characterized by three distinct regions, namely, region A where no switching occurs due to the fact that the adopted pulse width and amplitude are insufficient to reverse the polarization; region B where the switching has a certain probability to occur and an oscillatory behavior is registered among trials; and region C, where the switching occurs at every trial, i.e. the switching is deterministic.

B. Random Number Generation

The probabilistic ferroelectric switching observed in region B of Fig. 2(b) opens a completely new perspective for FeFET devices, reaching beyond their traditional memory application, which is only concerned with region C. Here, we propose to exploit the intrinsic switching variability for the true random number generation.

To this purpose, the gate pulse sequence in Fig. 1(b) is used again: after the initialization program pulse, the device is first set to a reference high-V_T state with $V_N = -4$ V, then a random program operation is performed by applying a pulse having the pulse width which corresponds to the probability of 50% for switching in Fig. 2(b). For the adopted pulse amplitude of 2.5 V, this pulse width is $t_{PW} = 9.1$ μs. In this way, the program transition tends to be induced only in half of the trial cycles. Finally, the transfer curve is read-out to assess the resulting V_T or the drain current state.

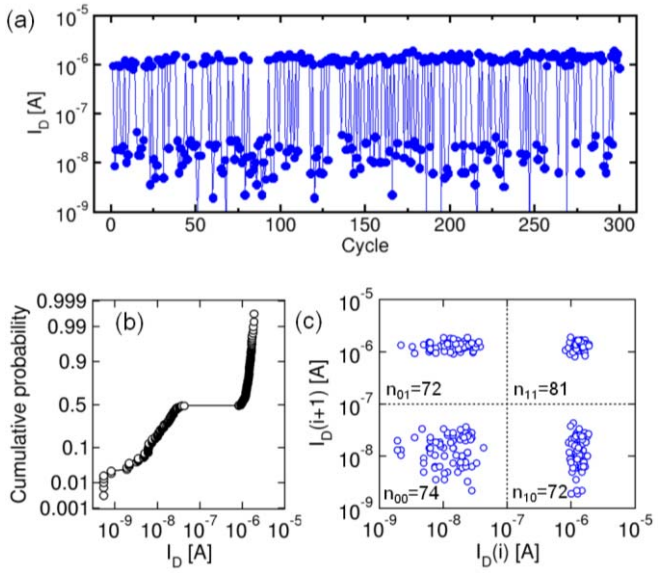

Fig. 3. (a) Drain current levels extracted at $V_G = 0$ V and sampled over 300 consecutive random programming operations using $t_{PW} = 9.1$ μs as the excitation pulse width. (b) Cumulative distribution plot of the obtained levels showing a bimodal distribution of states and an abrupt separation at $P = 0.4867$. Wider distribution for low I_D is an artifact due to limited measurement resolution. (c) Scatter plot of the drain current I_D at cycle $i+1$ as a function of I_D at cycle i indicating the existence of 4 populations ('00', '01', '10, and '11'), which are almost evenly represented in the obtained data set.

Fig. 3(a) shows the resulting drain current levels sampled over the consecutive 300 random program trials. It can be observed that the obtained bit stream has a binary form, with two current levels being clearly distinguishable and separated by almost two orders of magnitude. This can be understood by the aforementioned abrupt switching of these small devices and by the internal amplification effect inherent to the transistor operation. Consequently, a logical 'one' can be attributed to the low-V_T, and a logical 'zero' to the high-V_T state, without adopting an additional circuitry to separate the two states.

In order to preliminarily verify the apparent randomness of the obtained bits, we first evaluate whether the events of having a 'one' and a 'zero' are equally probable. Fig. 3(b) shows the cumulative probability of the states, revealing a clear bimodal distribution and a sharp transition at P = 0.4867. This indicates that there is 51.33% probability to find a '1' and 48.67% to find '0' in the output bit stream, which means that the predominance of one binary value over the other is negligible. Furthermore, the actual relationship between one number and its successor in a random sequence has no physical significance [16]. This implies that the output bit $i+1$ has to be independent of the previously generated bit i, or in general, independent of any previous bit. In other words, no correlation between the consecutive states in a generated sequence may occur [7]. In order to test this, we performed the correlation analysis by investigating $I_D(i+l)$ as a function of $I_D(i)$, where l is lag or bit distance and i runs from 1 to $300-l$. This resulted in four clearly distinguishable populations corresponding to four possible combinations of bits in this kind of a test, namely '00', '01', '10' and '11'. The populations were nearly equally represented in the set of data (with a probability close to 1/4), which means there is no preferential bit order. Fig. 3(c) shows exemplarily the relative scatter (lag) plot for $l = 1$. It is namely particularly important for FeFETs to ensure the absence of any correlation between adjacent states ($l = 1$). In this way, in fact, any kind of memory or imprint effects, which are known to afflict the ferroelectrics, could be excluded.

Although this work is primarily concerned with illustrating the novel concept of the FeFET based RNG, further aspects for a reliable and unbiased bit generation are of substantial interest as well. For instance, the stability of the operating point where P = 50%, which might be influenced by cycling or temperature, is essential. In fact, it is known that changes in operating temperature influence the ferroelectric switching [12], which might therefore cause an imbalance between the generated 'ones' and 'zeros'. This issue could be overcome by adopting real-time tracking mechanisms, as foreseen for other types of RNGs [9].

Finally, note that the bit generation rate can be tuned according to desired requirements. Considering that a linear increase in gate pulse amplitude leads to an exponential decrease of the switching time in FeFETs [12], the bit generation rate could be considerably increased by adopting a higher operating voltage.

III. Conclusion

In this letter, we have proposed a first implementation of a true random number generator based on a FeFET. It relies on the intrinsic switching variability of ultra-scaled FeFETs. The generated random bit stream contains a nearly unbiased sequence of 'ones' and 'zeros' and shows no memory effects among consecutive generation cycles. The results suggest FeFET as a promising technology for a compact on-chip entropy source for the RNG.

Acknowledgment

The authors would like to thank S. Müller and J. Ocker from FMC GmbH, J. Müller from Fraunhofer IPMS-CNT and colleagues from GlobalFoundries Dresden, Germany.

References

[1] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code*. Hoboken, NJ, USA: Wiley, 2007.

[2] R. Brederlow, R. Prakash, C. Paulus, and R. Thewes, "A low-power true random number generator using random telegraph noise of single oxide-traps," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2006, pp. 1666–1675, doi: 10.1109/ISSCC.2006.1696222.

[3] C. S. Petrie and J. A. Connelly, "A noise-based IC random number generator for applications in cryptography," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 47, no. 5, pp. 615–621, May 2000, doi: 10.1109/81.847868.

[4] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, "A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC," *IEEE Trans. Comput.*, vol. 52, no. 4, pp. 403–409, Apr. 2003, doi: 10.1109/TC.2003.1190581.

[5] N. Liu, N. Pinckney, S. Hanson, D. Sylvester, and D. Blaauw, "A true random number generator using time-dependent dielectric breakdown," in *Proc. Symp. VLSI Technol. (VLSIT)*, Jun. 2011, pp. 216–217.

[6] C.-Y. Huang, W. C. Shen, Y.-H. Tseng, Y.-C. King, and C.-J. Lin, "A contact-resistive random-access-memory-based true random number generator," *IEEE Electron Device Lett.*, vol. 33, no. 8, pp. 1108–1110, Aug. 2012, doi: 10.1109/LED.2012.2199734.

[7] S. Balatti, S. Ambrogio, Z. Wang, and D. Ielmini, "True random number generation by variability of resistive switching in oxide-based devices," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 5, no. 2, pp. 214–221, Jun. 2015, doi: 10.1109/JETCAS.2015.2426492.

[8] 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. Exp.*, vol. 7, no. 8, p. 083001, Jul. 2014, doi: https://doi.org/10.7567/APEX.7.083001

[9] W. H. Choi, Y. Lv, J. Kim, A. Deshpande, G. Kang, J.-P. Wang, and C. H. Kim, "A magnetic tunnel junction based true random number generator with conditional perturb and real-time output probability tracking," in *IEDM Tech. Dig.*, Dec. 2014, pp. 12.5.1–12.5.4, doi: 10.1109/IEDM.2014.7047039.

[10] J. Müller, E. Yurchuk, T. Schlösser, J. Paul, R. Hoffmann, S. Müller, D. Martin, S. Slesazeck, P. Polakowski, J. Sundqvist, M. Czernohorsky, K. Seidel, P. Kücher, R. Boschke, M. Trentzsch, K. Gebauer, U. Schröder, and T. Mikolajick, "Ferroelectricity in HfO_2 enables nonvolatile data storage in 28 nm HKMG," in *Proc. Symp. VLSI Technol. (VLSIT)*, Jun. 2012, pp. 25–26, doi: 10.1109/VLSIT.2012.6242443.

[11] M. Trentzsch, S. Flachowsky, R. Richter, J. Paul, B. Reimer, D. Utess, S. Jansen, H. Mulaosmanovic, S. Müller, S. Slesazeck, J. Ocker, M. Noack, J. Müller, P. Polakowski, J. Schreiter, S. Beyer, T. Mikolajick, and B. Rice, "A 28 nm HKMG super low power embedded NVM technology based on ferroelectric FETs," in *IEDM Tech. Dig.*, Dec. 2016, pp. 11.5.1–11.5.4, doi: 10.1109/IEDM.2016.7838397.

[12] H. Mulaosmanovic, J. Ocker, S. Müller, U. Schroeder, J. Müller, P. Polakowski, S. Flachowsky, R. van Bentum, T. Mikolajick, and S. Slesazeck, "Switching kinetics in nanoscale hafnium oxide based ferroelectric field-effect transistors," *ACS Appl. Mater. Interfaces*, vol. 9, no. 4, pp. 3792–3798, Jan. 2017, doi: 10.1021/acsami.6b13866.

[13] H. Mulaosmanovic, S. Slesazeck, J. Ocker, M. Pesic, S. Müller, S. Flachowsky, J. Müller, P. Polakowski, J. Paul, S. Jansen, S. Kolodinski, C. Richter, S. Piontek, T. Schenk, A. Kersch, C. Kunneth, R. van Bentum, U. Schroder, and T. Mikolajick, "Evidence of single domain switching in hafnium oxide based FeFETs: Enabler for multi-level FeFET memory cells," in *IEDM Tech. Dig.*, Dec. 2015, pp. 26.8.1–26.8.3, doi: 10.1109/IEDM.2015.7409777.

[14] J. Müller, T. S. Boscke, U. Schroder, R. Hoffmann, T. Mikolajick, and L. Frey, "Nanosecond polarization switching and long retention in a novel MFIS-FET based on ferroelectric HfO_2," in *IEEE Electron Device Lett.*, vol. 33, no. 2, pp. 185–187, Feb. 2012, doi: 10.1109/LED.2011.2177435.

[15] H. Mulaosmanovic, J. Ocker, S. Müller, M. Noack, J. Müller, P. Polakowski, T. Mikolajick, and S. Slesazeck, "Novel ferroelectric FET based synapse for neuromorphic systems," in *Proc. Symp. VLSI Technol. (VLSIT)*, Jun. 2017, pp. T176–T177, doi: 10.23919/VLSIT.2017.7998165.

[16] D. E. Knuth, *Art of Computer Programming: Seminumerical Algorithms*, vol. 2, 2nd ed. Reading, MA, USA: Addison-Wesley, 1981.