Exploiting FeFET Switching Stochasticity for Low-Power Reconfigurable Physical Unclonable Function

Xinrui Guo, Xiaoyang Ma, Franz Müller[#], Ricardo Olivo[#], Juejian Wu, Kai Ni^{*}, Thomas Kämpfe[#], Yongpan Liu, Huazhong Yang, and Xueqing Li BNRist/ICFC, EE Department, Tsinghua University; ^{*} Rochester Institute of Technology; [#] Fraunhofer IPMS Corresponding Email: xueqingli@tsinghua.edu.cn, thomas.kaempfe@ipms.fraunhofer.de, Kai.Ni@rit.edu

Abstract—This paper investigates reconfigurable physical unclonable function (PUF) design by exploiting the polarization switching variation and stochasticity in ferroelectric field-effecttransistors (FeFETs). The proposed PUFs include 1transistor/cell (1T/C) and 2T/C designs. The denser 1T/C PUF splits random '0' and '1' states using a tactically pre-defined reference. The 2T/C PUF needs no dedicated references and obtains unbiased random states by differentiating two FeFETs under a proposed sensing error cancellation scheme. Experimental measurements have shown the uniform randomness, uniqueness, repeatability and reconfigurability of the response. Further simulations using an experimentally calibrated multi-domain FeFET model show high energy efficiency and robustness on design parameters.

Keywords—Physical unclonable function, FeFET, hardware security, stochasticity, reconfigurable PUF, offset cancellation.

I. INTRODUCTION

Physical unclonable function (PUF) is a critical hardware security primitive in key generation and device authentication to counter possible security threats [1]. As shown in Fig. 1(a), the PUF provides a physical system, mapping a given challenge input to some specific and unpredictable response as a digital fingerprint. To achieve security purposes, the unpredictable randomness and uniqueness of the responses are critical for a PUF design. Meanwhile, the general specifications, e.g., power, latency, and density, are also important in practice. Furthermore, applications may require a PUF to be reconfigurable [2].

In prior works, CMOS manufacturing process variations have been explored for PUF design, including the ring-oscillator PUF, arbiter PUF, SRAM PUF, etc., born with good compatibility with other circuits. However, they suffer from relatively low area efficiency. Meanwhile, cycle-to-cycle variation is not significant in these designs, thus it is challenging to achieve high reconfigurability. Non-volatile memories (NVMs) provide a new option for reconfigurable PUF design by exploiting the randomness from the internal device operating mechanism as the entropy source [2]-[5]. While NVM-based PUF designs have led to higher reconfigurability, the enrollment and authentication steps still suffer from relatively high power consumption due to the memory access characteristics.

Recently, HfO₂-based ferroelectric field-effect transistors (FeFETs) are emerging as a promising NVM candidate, thanks to the compatibility with the advanced CMOS process, ultra-low power consumption, a high on-off ratio, moderate operating voltage and moderate endurance [6]-[9]. For FeFETs, the drain-source current is modulated by the ferroelectric polarization, and reports have revealed the polarization switching stochasticity and variation [7]-[8]. This makes FeFETs intriguing for low-power, reliable and reconfigurable PUF and true random number generators.

In this paper, we investigate the FeFET-based PUF design space, and propose two low-power reconfigurable FeFET-based PUF structures targeting at different applications as shown in Fig. 1(c-d), naming one-transistor-per-cell (1T/C) structure and 2T/C structure, together with the associated programing and sensing techniques. The simulation and experimental results show excellent PUF performance for both proposed designs, including uniform randomness, uniqueness, reliability and reconfigurability. Also, robustness to design parameters and high energy efficiency are confirmed by further simulation results.



Fig. 1. Proposed FeFET PUF: (a) PUF concept; (b) array implementation; (c) 1T/C with pre-defined reference; (d) 2T/C with SA offset cancellation.

II. NEW OPPORTUNITIES WITH FEFET PUF

A. FeFET basics

In 2011, HfO₂-based materials were found to exhibit ferroelectricity [10]. This is a nice ferroelectric replacement with mature compatibility with the CMOS technology, including FinFET technologies. Following works integrated the HfO₂-based ferroelectric layers in the MOSFET gate stack successfully, as shown in Fig. 2(a) [8]. The FeFET scalability has been demonstrated by recent sub-10nm fin-structure FeFETs [9].

A critical part of FeFET is the ferroelectric layer. Actually, the layer can contain multiple ferroelectric domains, whose polarization switching has been observed experimentally [7]. The domains may stay at either positive or negative polarization, thus leading to different integrated polarization charges at the internal gate. Accordingly, the sensed drain-source current I_{DS} varies with different V_{th}, as shown in Fig. 2(b).



Fig. 2. FeFET background (data from [8]): (a) a device structure; (b) domains of different polarization; (c) variation and switching stochasticity; (d) accumulated switching probability.

B. Why FeFETs are promising for PUF design?

There are several essential metrics to evaluate the PUF behavior: normalized response Hamming Weight (HW, ideally 50%) for uniform randomness, normalized inter-chip Hamming Distance (HDinter, ideally 50%) for uniqueness, and normalized intra-chip Hamming Distance (HDintra, ideally 0%) for repeatability. The PUF entropy source would affect the above metrics directly or indirectly.

Till now, many NVM-based PUF designs have been proposed, including RRAM, PCM, STT-MRAM PUF, etc. [2]-[5]. These designs use the device-to-device (D2D) and cycle-to-cycle (C2C) variations or stochasticity from the internal device operating mechanism, enabling high reconfigurability more easily than traditional CMOS-based PUFs. Prior RRAM PUF uses the stochastic switching mechanism and intrinsic RRAM state variability [2]. FeRAM, PCM, and STT-MRAM could also be used for PUF design, benefiting from the inherent random process parameter variability and programing sensitivity [3]-[5]. However, these PUFs consume significant power and result in relatively low energy efficiency in every reconfigure cycles.

Interestingly, it has been observed that the switching behavior of one single domain in FeFETs is an abrupt and stochastic process, regulated by the electric field across the domain. Fig. 2(c) gives the experimental results of the device variation caused by stochastic switching, and Fig. 2(d) shows the cumulative switching probability of the ferroelectric domains [8]. The device mechanism indicates that FeFETs could reach slightly different total polarization states even after application of similar write pulse. Also, the quantity of the domains can affect the variability of I_{DS} . These internal mechanisms enable FeFETs to behave as an entropy source for security purposes including PUF and true random number generators, while it could be a challenge for traditional general-purpose memory applications.

Compared with these existing PUF solutions, our FeFET-based solution is promising because of these new opportunities: (i) ultralow power consumption and massive parallel initialization capability because of the capacitive write-access load; (ii) controllable switching stochasticity to achieve excellent PUF performance; (iii) significantly high on-off ratio (>10⁴) providing a higher noise margin and lower sensing costs; (iv) the FeFET is a three-terminal transistor with an extra gate control, benefiting read and write isolation and convenient access.

III. PROPOSED FEFET-BASED 1T/C AND 2T/C PUF DESIGNS

A. Proposed 1T/C PUF

The proposed 1T/C PUF circuit structure has been illustrated in Fig. 1(b-c). Here, 1T/C means that each PUF bit is generated from one FeFET. The four-step PUF enrollment flow is illustrated in Fig. 3(a) and described below.



Fig. 3. The enrollment flow of the proposed PUFs: (a) 1T/C; (b) 2T/C.

Step I – Initialization: all cells in the FeFET array are enforced to state '0'. This can be done simultaneously for the whole array, while the other existing NVM PUFs cannot due to driving load limitations.

Step II – Stochastic Switching: a pre-defined write pulse is applied to all cells, such that they may switch their ferroelectric polarization probabilistically. This step can also be done under high array-level

parallelism due to the DC-power-free FeFET write features, which is also challenging in other NVM-based PUFs.

Practically, limited by the resolution of sensing the FeFET drain current, it is preferred to make the polarization state distribution wide such that the entropy source generated from the switching mechanism is fully exploited. Luckily, the pulse amplitude and duration could vary in a large range and still generate a quite wide distribution, confirmed by the results in Section IV.

Step III – Reference Search: the reference I_{DS} is used as a threshold to identify '0' and '1' states after step II. Intuitively, it plays a critical role in ensuring the PUF uniform randomness.

In practice, other circuit and process non-idealities such as the sense amplifier (SA) offset, environmental changes (e.g., temperature and the EM field), device aging, etc., force the actual I_{DS} deviate from prior knowledge, and thus cause PUF performance degradation. To achieve the I_{DS} reference accuracy, an adaptive reference I_{DS} search approach borrowed from data converters is adopted, namely the successive-approximation-register (SAR) search, as shown in Fig. 4(a). The SAR search carries out a recursive procedure to approach the desired resolution quickly, as the example given in Fig. 4(b).



Fig. 4. Reference I_{DS} SAR search approach: (a) flow chart; (b) an example.

Step IV - Re-programing: the re-programing operation sets the polarization state of the '1' / '0' cells to strong positive / negative, increasing the polarization difference between the two states. This leads to a larger noise margin for both read and standby operations, beneficial for both reliability and sensing efficiency. An example of the state distribution and data pattern is shown in Fig. 5. After the re-programing, the ratio between the average '1' current and '0' current is increased by 976x (from 1.23 to 1200).



Fig. 5. FeFET PUF states: a simulation example. (a-b) I_{DS} distribution before / after re-programing; (c) An I_{DS} data pattern example of 100 128-bit PUFs after write pulse without re-programing; (d) Re-programed digital response.

B. Proposed 2T/C PUF

As discussed above, to account for the I_{DS} distribution deviation, the *Reference Search* step in 1T/C PUF enrollment flow takes noticeable latency and energy consumption. Inspired by the RRAM PUF in [2], using two FeFETs in one cell could largely eliminate the impact of I_{DS} distribution deviation by sensing I_{DS1}-I_{DS2} rather than absolute I_{DS}. The zero expected mean value of I_{DS1}-I_{DS2} makes it no more necessary to find a dedicated reference for enrollment.

The 2T/C PUF circuit structure is shown in Fig. 1(d), and the enrollment flow is shown in Fig. 3(b). The enrollment flow consists of unchanged steps (i)(ii), and the different step (iii) naming

differential sensing and re-programing. Here each pair of FeFET I_{DS} is sensed by a differential SA, and the result is written back for an enhanced noise margin. Since both cells are written back, the noise margin is doubled compared with 1T/C design. Furthermore, the symmetric structure could effectively avoid side-channel attacks.

A non-negligible issue in the 2T/C design is the SA offset. Considering the SA offset impact directly adding up to the current in one input port, the number of '1' / '0' cells deviates accordingly, as the error zone shown in Fig. 6(a). In an extreme case when the SA offset is larger than the maximum absolute I_{DS} difference (unlikely to happen), the output will always be '1' or '0'. To tackle the SA offset issue, we borrow the idea of "chopper SA" design in high-definition audio amplifiers to compensate the SA offset, as illustrated in Fig. 1(d) and re-drawn in Fig. 6(c). The idea is straightforward: the SA offset adds a fixed constant to one input port, so alternatively switching the differential SA input ports (V_{IN}+ \Leftrightarrow V_{IN}-) and also output ports (V_{OUT}+ \Leftrightarrow V_{OUT}-) could average out the SA offset impact over time with minor overhead.



Fig. 6. SA offset impact on 2T/C PUF: without / with offset cancellation.

Comparing the two design structures, the 1T/C design is denser in a cell layout with extra counting and reference adjusting circuits. The 2T/C PUF outperforms with reference-free enrollment by using density in exchange for calculation overhead. Therefore, the former design is suitable for the applications under strict area limitation and sufficient computing resources; the latter is suitable for fastreconfiguration scenarios with less area restrictions.

C. Reconfigurability

Another highlight is the high reconfigurability of the two proposed designs. Different from traditional CMOS-based PUFs with almost fixed entropy source, the proposed designs use the randomness from an internal device mechanism, leveraging high reconfigurability due to C2C stochasticity. Once required, reconfiguration can be initiated simply by re-running the enrollment steps. The high reconfigurability enhances the PUF security level, since the possible information leakage between the reconfiguration cycles may not be sufficient upon adversary attacks.

IV. FEFET-BASED PUF EVALUATION

A. Evaluation settings

Experimental Settings. To verify the functionality of the proposed PUF design, we are utilizing HfO₂ based FeFETs which are integrated into the 28nm super low power technology platform with a gate area of 500x500nm². The TEM image and I_{DS}-V_G measured curves of the device is given in Fig. 7(a). By harnessing the partial polarization switching under different write pulse amplitudes, a 2-bit storage in FeFET is achieved under single pulse write operation. Specifically, the devices are programmed into low-V_{th} state by applying a gate voltage of 4.5V for 500ns and into high-V_{th} state by applying -5V for 500ns. To obtain an intermediate state we apply 3V for 500ns onto a device, which is prior programmed into high-V_{th} state.

FeFET model for simulation. The comprehensive multi-domain FeFET model proposed in [8] is used for accurate simulations. The model captures the device scalability, variation, stochasticity, and accumulation of the ferroelectric behaviors, and has been carefully calibrated with measured metal-ferroelectric-metal (MFM) structure characteristics from the foundry samples.

Default simulation parameters. The ferroelectric layer thickness is 8nm by default. The number of ferroelectric domains is set to 200 for typical evaluations. The simulation programing gate pulse is 3.4V, $3.0\mu s$. The read-out gate voltage is 1.0V, which could be increased for larger sensed current. The SA offset is set to 1.0% of average I_{DS} to reflect circuit non-idealities, unless otherwise stated.

B. Uniform randomness, uniqueness, repeatability and reconfigurability: simulation and experimental results

As shown in Fig. 7(b-c), simulation and experimental results show that both PUF designs exhibit excellent uniform randomness, uniqueness and repeatability. In simulation results, 1,000 128-bit PUF samples give 50.00% and 50.11% μ (HW) for 1T/C and 2T/C designs, respectively; and μ (HDinter) is almost ideally located at 50.01% and 49.95%, with standard deviation as low as 4.35% and 4.37% for two proposed designs, respectively. Although FeFET fabrication is in its early infancy, we still obtained 60 samples in 28nm process successfully. The experimental measurements of these samples have shown near-ideal results with μ (HDinter) located at 51.1% and 53.3%, for 1T/C and 2T/C designs, respectively. It could be even closer to the ideal 50% with more samples.

To show high response repeatability of the proposed designs, 20 experimental read operations were performed repeatedly, under 25°C. No error was detected from the measurements, thanks to the long retention time and the large noise margin widened by reprograming. It is thus promising to keep the ultra-low BER, and HDintra very close to the ideal value 0%.

High reconfigurability is also confirmed for both designs. Fig. 7(d) shows the sensed current of four FeFET PUF cells during 10 reconfiguration cycles, three from simulation and one from experiment, indicating the independence in history configurations. The correlation matrixes of 50 reconfigured 1T/C and 2T/C responses from simulations are shown in Fig. 7(e-f), respectively, indicating little correlation between reconfiguration cycles, and thus high reconfigurability for both designs.



Fig. 7. PUF evaluation. (a) FeFET TEM image and I_{DS} -V_G curves of 60 devices, under different Vth; (b-c) HW and HD results of 1T/C and 2T/C designs; (d) Sensed I_{DS} of 4 FeFET cells in 10 cycles; (e-f) Correlation matrix of 50 reconfigured 1T/C and 2T/C PUF responses.

C. Robustness to parameters: further simulation results

We adopted further simulations to explore the impact of various parameters on PUF performance. Each set of simulations below is completed on 100 128-bit PUF samples.

1) Impact of write pulse amplitude and duration

Fig. 8 shows the impact of programing pulse amplitude and duration. From {Amp=3.4V, $Dur=3\mu s$ } to {Amp=4.0V, $Dur=9\mu s$ }, the average I_{DS} of the FeFETs increases from 2.46µA to 3.85µA, and μ (HDinter) varies around 50% with less than 0.12% deviation, showing high robustness against the programing pulse parameters.



Fig. 8. IDS and HDinter with varying write pulse amplitude and duration.

2) Impact of ferroelectric domain number

As revealed in related works, the FeFET switching behavior varies with the number of ferroelectric domains. Therefore, to incorporate the impact of the reduced number of ferroelectric domains, especially in scaled small devices, simulations are carried out with the domain number equal to 20, 200, and 2,000.

Table I summarizes the PUF evaluation results. The simulations are carried out with the practical consideration of error sources under normal and worse cases: reference I_{DS} errors up to 1% for 1T/C PUF (considering non-ideal reference I_{DS} search) and the SA offset up to 5% for the 2T/C PUF. Results show that the PUF performance is robust with the domain number varying between 20 and 2000.

In addition, from the results with 1% reference I_{DS} error and 5% SA offset, the 20- and 200-domain cases provide higher performance. This is because, compared with the 2000-domain FeFETs, less ferroelectric domains lead to an extended I_{DS} distribution with wider variations under the same write pulse. Therefore, the PUF performance may improve with the sensing errors being comparatively smaller to the I_{DS} distribution range. This phenomenon indicates that the proposed PUF designs fit very well with the scaling trend, as generally smaller FeFET devices contain less ferroelectric domains. Meanwhile, for many-domain devices, e.g. the 2000-domain FeFETs, reducing the sensing errors is an effective method to keep satisfying performance.

TIBLET MILLET OF QUALITY OF TERMOLEDETING BOMMIND							
Domain Number	20	200	2000	20	200	2000	
Normal Case	1T/C (0% reference I _{DS} error)			2T/C (1% SA offset)			
$\mu(HW)$	50.0%	50.0%	50.0%	49.2%	49.8%	49.8%	
μ (HDinter)	49.9%	50.0%	50.1%	49.8%	50.0%	50.0%	
σ (HDinter)	4.43%	4.44%	4.41%	4.44%	4.37%	4.53%	
Worse Case	1T/C (1% reference I _{DS} error)			2T/C (5% SA offset)			
$\mu(HW)$	50.8%	53.0%	59.9%	49.3%	49.8%	50.1%	
μ (HDinter)	49.9%	49.8%	48.0%	49.8%	49.9%	50.4%	
σ (HDinter)	4.43%	4.46%	4.39%	4.46%	4.79%	20.6%	

TABLE I IMPACT OF QUANTITY OF FERROELECTRIC DOMAINS

3) Impact of ferroelectric layer thickness

The ferroelectric layer thickness (t_{FE}) affects the polarization switching in two critical ways:

(i) *The switching possibility*: as the polarization switching behavior is regulated by the electric field, the change of the ferroelectric layer thickness (t_{FE}) affects the capacitance, the voltage drop, and further, the electric field under the same external driving voltage.

(ii) *Ferroelectric domain number and size*: it is reported that the ferroelectric domains of thin films follow the Landau-Lifshitz-Kittel (LLK) scaling that the ferroelectric domain width is proportional to $t_{FE}^{0.5}$ [11]. Different scaling exponents have also been reported, illustrating complicated relationship between t_{FE} and the ferroelectric domain size [12]. In general, the domain size decreases with a smaller t_{FE} , leading to more domains in a transistor of the same size.

Fig. 9 shows the impact of t_{FE} under default programing settings. μ (HDinter) aligns well to 50% with less than 0.17% deviation, exhibiting the robustness in different FeFET processes.



Fig. 9. Impact of t_{FE} with $\sigma(t_{FE})=0.32$ nm: (a-b-c) $t_{FE}=6$ nm, 8nm, 10nm.

D. Energy and latency performance

As listed in Table II, the average enrollment energy and authentication energy are 85.1fJ/bit and 1.75fJ/bit for the proposed 1T/C PUF, respectively, and 53.1fJ/bit and 1.75fJ/bit for 2T/C PUF, respectively. Although some data were not well reported in prior works, the PUF enrollment energy efficiency of the proposed work

is much higher than other reported achievements. One reason is the DC-power-free write access to FeFETs. The enrollment latency is evaluated to be at μ s level, which could be improved with the FeFET technology or using a higher voltage (using more write energy). For authentication, the energy efficiency of FeFET PUFs is also among the best due to a large on-off ratio and a DC-free read operation.

TABLE II ENERGY & LATENCY COMPARISON OF REC	ENT WORKS
---	-----------

Operations	Enrollment		Authentication		
Specifications	Energy	Latency	Energy	Latency	
1T/C FeFET PUF	85.1fJ/bit	3.22µs/row	1.75fJ/bit	1ns/row	
2T/C FeFET PUF	53.1fJ/bit	3.20µs/row	1.75fJ/bit (1FeFET)	1ns/row	
RRAM [2]	3028fJ/bit	-	>fJ/bit ^a	${\sim}10 ns^{a}$	
PCM-RAM [4]	450fJ/bit	0.150µs	>fJ/bit ^a	${\sim}10 ns^{a}$	
STT-MRAM [5]	630fJ/bit	0.040µs	>fJ/bit ^a	10ns	

^a: only a typical memory read operation included; reference data from [13].

V. CONCLUSION

This paper has proposed two FeFET-based reconfigurable PUF designs targeted at different scenarios, and the workflow have been presented and discussed. Comprehensive evaluations with experimental measurements have shown the promise for parameter-robust low-power reconfigurable PUF applications. In addition, it is noted that the proposed designs belong to the category of weak PUFs. Future extension to strong PUFs is also valuable.

VI. ACKNOWLEDGMENTS

This work is partly supported by NSFC #61874066, #61720106013, and the ECSEL Joint Undertaking in collaboration with the European Union's H2020 Framework Program (H2020/2014-2020) and National Authorities, under grant agreement number 826655. We thank Globalfoundries for the provision of 28nm technology FeFET structures.

REFERENCES

- C. Herder et al, "Physical Unclonable Functions and Applications: A Tutorial," in *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126-1141, 2014.
- [2] Y. Pang et al., "25.2 A Reconfigurable RRAM physically unclonable function utilizing post-process randomness source with <6×10-6 native bit error rate," 2019 IEEE International Solid-State Circuits Conference - (ISSCC), San Francisco, CA, USA, 2019, pp. 402-404.
- [3] J. A. Rodriguez et al, "Physical unclonable function system and method," U.S. Patent 10,424,361, issued September 24, 2019.
- [4] L. Zhang et al, "Exploiting process variations and programming sensitivity of phase change memory for reconfigurable physical unclonable functions," in *IEEE Transactions on Information Forensics* and Security, vol. 9, no. 6, pp. 921-932, June 2014.
- [5] L. Zhang et al, "Highly Reliable Spin-Transfer Torque Magnetic RAM-Based Physical Unclonable Function With Multi-Response-Bits Per Cell," in *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1630-1642, Aug. 2015.
- [6] T. S. Böscke et al, "Ferroelectricity in hafnium oxide: CMOS compatible ferroelectric field effect transistors," 2011 IEDM, pp. 24.5.1-24.5.4.
- [7] H. Mulaosmanovic et al., "Evidence of single domain switching in hafnium oxide based FeFETs: enabler for multi-level FeFET memory cells," 2015 IEEE International Electron Devices Meeting, 2015, pp. 26.8.1-26.8.3.
- [8] S. Deng et al, "A comprehensive model for ferroelectric FET capturing the key behaviors: scalability, variation, stochasticity, and accumulation," in 2020 IEEE Symposium on VLSI Technology, June 14-19, 2020.
- [9] A. Sharma et al, "1T nonvolatile memory design using sub10nm ferroelectric FETs," *IEEE EDL*, vol. 39, no. 3, pp. 359–362, 2018.
- [10] T. S. Böscke et al, "Ferroelectricity in hafnium oxide thin films," Appl. Phys. Lett., vol. 99, no. 10, pp. 102903, Sep. 2011.
- [11]L. Landau et al, "3 On the theory of the dispersion of magnetic permeability in ferromagnetic bodies," in *Perspectives in Theoretical Physics*, L. P. Pitaevski, Ed. Amsterdam: Pergamon, 1992, pp. 51–65.
- [12] L. Chen et al., "Thickness dependence of domain size in 2D ferroelectric CuInP2S6 nanoflakes," *AIP Advances*, vol. 9, no. 11, p. 115-211. 2019.
- [13] S. Salahuddin et al, "The era of hyper-scaling in electronics," *Nature Electron.*, vol. 1, no. 8, pp. 442-450 2018.