DWM-PUF: A Low-Overhead, Memory-based Security Primitive

Anirudh Iyengar
Computer Science and Engineering
University of South Florida
anirudh@mail.usf.edu

Kenneth Ramclam
Computer Science and Engineering
University of South Florida
kramclam@mail.usf.edu

Swaroop Ghosh
Computer Science and Engineering
University of South Florida
sghosh@cse.usf.edu

Abstract*—Physically Unclonable Function (PUF) is a security primitive to address hardware security issues such as chip authentication, Intellectual Property (IP) protection etc. Conventional CMOS PUFs are built on delay (inverter chains, scan chains etc.) or memory structures (like SRAM). In this paper, we propose a novel PUF which works on the principles of spintronic Domain Wall Memory (DWM). Conventional DWM is limited by pinning due to process variations induced surface roughness of the nanowire. We exploit this limitation towards chip-authentication. We propose two flavors of PUFs namely relay-PUF and memory-PUF. The proposed PUFs show excellent entropy (measured by Hamming Distance). We also analyze metrics such as robustness, area and power of the DWM-PUFs. The memory-PUF indicated up to an order of magnitude reduction in power compared to SRAM PUF.

***Keywords*— Domain Wall Memory; Hardware Security; Physically Unclonable Function; Spintronic PUF; DWM-PUF.**

I. INTRODUCTION

A. Physically Unclonable Functions

The manufacturing of the present day integrated circuits (IC) are mostly outsourced to external companies. Under this business model the design is exposed to tampering and cloning by the third party breaching the Intellectual Property (IP). IC cloning also siphons off the economic benefits of the product. Due to high tech facilities employed by adversaries, isolating the fake chips from the genuine ones is becoming increasingly difficult task. Traditionally, unique keys are generated by the ICs for important applications such as IP security, counter-plagiarism etc. These keys are then stored on the on-chip non-volatile memory that is thought to be impervious to illegal access and duplication. However adversaries can decode the secret key through Reverse Engineering (RE). The duplicated chip with the key obtained through RE cannot be distinguished from genuine chip. In order to address these issues an auxiliary circuit i.e. Physically Unclonable Function (PUF) is incorporated in the authentic chips. PUFs are designed to exploit the physical properties of the chip (e.g., process) to generate its unique identification key. PUF is unclonable as the duplicate of this circuit will not provide the same identification tag as original even if the ICs are functionally identical. PUFs work on the foundation of challenge-response protocol, which functions on the basis of complex and variable physical process.

B. Types of PUFs

PUFs fall under two basic categories: electronic and non-electronic [19]. Electronic PUF's are based on electronic properties that determine the challenge-response protocols, such as gate delay, threshold voltage switching times etc. The most popular ones are: Arbiter PUF [1-2], Ring Oscillator PUF [1-4] and SRAM PUF [5]. The nano-electronic PUFs e.g., memristor based PUF [6-11] is also investigated due to its enhanced security feature. The non-electronic PUFs e.g., optical PUF, magnetic PUF, and acoustical PUF [19] use non-electrical challenge-response mechanism for their operation.

Conventional CMOS PUFs suffer from power, limited randomness offered by silicon substrate and restricted number of challenge-response pairs. This brings the need to investigate emerging technologies such as memristors, spintronic devices etc. The experimental results on spin valves, magnetic-tunnel junctions (MTJ), domain wall memory (DWM) etc. [12-18] have created enormous interest in spin based computations. The most promising effect is current induced modulation of magnetization dynamics discovered in MTJ and DWM as it opens door to energy-efficient logic and memory design. Interaction between injected current and local magnetization creates several Spin-Transfer Torque (STT) mechanisms that are excellent sources of entropy in the magnet. We note that the nonlinear dynamics of domain walls (DWs) in the physical magnetic system can be leveraged for hardware security and authentication. *To the best of our knowledge, this is the first effort towards employing spintronics for designing PUFs*. The primary contributions of this paper are as follows:

- We provide analysis of DW pinning in the nanowire (NW) due to process variations.
- We propose two flavors of PUF models that exploit DW pinning and offer higher degree of randomness.
- Our investigation revealed that DWM PUF can be effective in generating unique identification keys at the cost of low-power consumption.
- We also propose novel approaches to expand challenge-response pairs which are unique to DWM.

The rest of the paper is organized as follows. We describe the background on DWM and pinning effect in Section II. The proposed PUF designs and simulation results are described in Section III. Conclusions are drawn in Section IV.

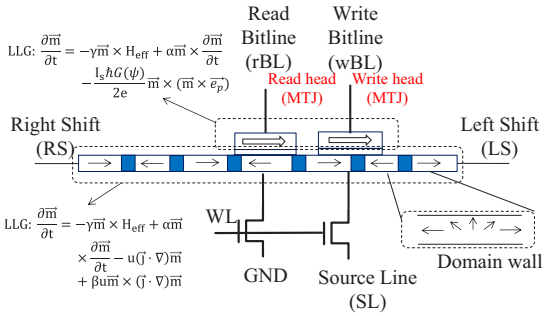
II. BASICS OF DWM

In this Section, we provide the basics DWM and the impact of process variation on DW pinning. We also establish the relationship between variation induced pinning and PUF design.

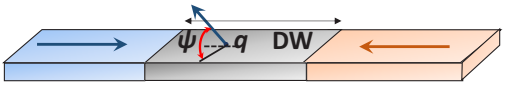
A. Brief Introduction

Magnetic memory is promising due to its high-density, low-power and non-volatility. DWM is a flavor of magnetic memory that provides the above benefits due to its ability to store multiple bits per bitcell for high-density [12-14]. Additionally,

978-1-4799-4112-4/14/$31.00 ©2014 IEEE



(a)



(b)

Fig. 1. (a)Schematic of DWM and governing equations and, (b) definition of q & ψ.

it provides low standby power (due to non-volatility), fast access, good endurance and retention [15]. DWM consists of three components: (a) write head, (b) read head and, (c) magnetic nanowire (Fig. 1(a)). The read and write heads are similar to conventional MTJ whereas NW holds the bits in terms of magnetic polarity. The most interesting effect in the NW is the formation of DW between domains of opposite polarities. The dynamics of NW is governed by the dynamics of DW. The DWs can be shifted forward and backward by injecting charge current from left-shift (LS) and right-shift (RS) contacts. In essence, the NW is analogous to a shift register. The new domains are injected by first pushing current through shift contacts to move the bits in lockstep fashion in order to bring the desired bit under write head. Next spin polarized current is injected through write MTJ (using wBL and SL) in positive or negative direction to write a '1' or '0' (up-spin or down-spin) in the NW. Read is performed by bringing the desired bit under the read head using shift and sensing the resistance of MTJ formed by DW under the read head (using rBL). It can be noted that this new access mechanism makes shifting of DWs critical to the functionality of the memory. The robustness, speed and power consumption of the memory has a significant dependency on DW dynamics. Various factors affect the DW motion such as shift current magnitude, phase and physical properties of the NW. The DW position and tilt angle is determined by solving the Landau-Liftshitz Gilbert (LLG) equation which is a torque balancing equation (Fig. 1(b)).

$$\frac{\partial \vec{m}}{\partial t} = -\gamma \vec{m} \times \overrightarrow{H_{eff}} + \alpha \vec{m} \times \frac{\partial \vec{m}}{\partial t} - u(\vec{j} \cdot \nabla)\vec{m} + \beta u \vec{m} \times (\vec{j} \cdot \nabla)\vec{m}$$

Where $\vec{m}$ and $\vec{j}$ are unit vectors representing local magnetic moment of DW and current flow respectively, $\overrightarrow{H_{eff}} = -\frac{1}{\mu_0 M_s}\frac{\delta w}{\delta \vec{m}}$ is the effective field, α is damping constant, β is non-adiabatic spin torque transfer term and u is a scalar quantity having the units of velocity. Term u depends on the current density J, the spin polarization P, saturation magnetization M_s and Bohr Magneton μ_B as follows:

$$u = \frac{\mu_B J P}{e M_s}, \mu_B = \frac{\hbar e}{2 m_e}$$

TABLE I. MAGNETIC CONSTANTS USED FOR DW DYNAMICS

Parameter	Value
α	Varied (0.01 - 0.02)
β	Varied (0.0 - 0.1)
Bohr magneton(μ_B)	$9.27e^{-24}$ J/T
M_s	$8e^5$ A/m
Exchange Constant (A)	$1.3e^{-11}$ J/m.
Length(l)/Width(w)/Thickness(t) of NW	$1e^{-6}$ m/$100e^{-9}$ m/$10e^{-9}$ m
ϒ	$1.76e^{11}$ /G s
Demagnetization Field (Hk)	1600~1800 Oe.

In the above expression, $\hbar$ is reduced plank's constant, e is electron charge and m_e is electron mass. The final expressions of motion are given by [17]

$$(1+\alpha^2)\dot{q} = \frac{\mu_0}{2}\gamma\Delta(H_k \sin 2\psi - \pi H_T) + \alpha\Delta\gamma\left(\mu_0 H_A - \frac{Vq}{M_s d}\right) + (1+\alpha\beta)u$$

$$(1+\alpha^2)\dot{\psi} = -\frac{\mu_0}{2}\alpha\gamma(H_k \sin 2\psi - \pi H_T) + \gamma\left(\mu_0 H_A - \frac{Vq}{M_s d}\right) + \frac{\beta-\alpha}{\Delta}u$$

Where, $\dot{q}$ and $\dot{\psi}$ are the time derivatives of the domain wall position and tilt angle respectively. We model the position (q) and tilt angle (ψ) of DW using Verilog-A. With constants provided in Table 1.

B. *Process Variation Modeling and Analysis*

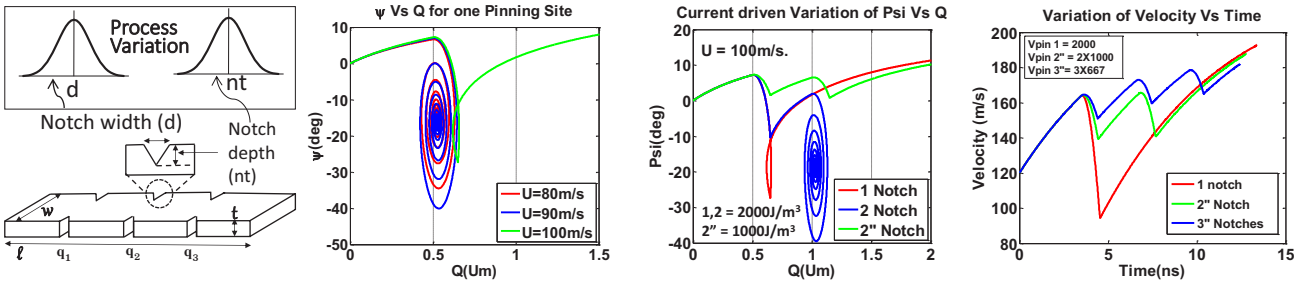
Note that the above expressions don't consider the effect of process variation induced roughness of the NW on the DW dynamics. The variations in the NW could create unwanted physical notches that could pin the DW or degrade its velocity. The magnitude of pinning energy is dependent on notch dimensions (Fig. 2(a). We model the pinning energy as follows [16-17]:

$$\sigma_{pin} = \frac{V(q-q_{pin})^2}{M_s(2d)} \quad \begin{cases} V = V_{pin} & q_{pin} - d \le q \le q_{pin} + d \\ V = 0 & otherwise \end{cases}$$

Where q_{pin} is the pinning site, V_{pin} is the pinning potential at that particular location and d is pinning width. Multiple pinning sites are modeled by changing q_{pin} accordingly. The LLG is solved with the pinning sites in order to observe the impact of DW dynamics.

In practice, several techniques have been suggested to mitigate the effect of variations [20]. However, we demonstrate that it can be exploited to generate challenge-response pairs for authentication. To understand the impact of variations we conduct two experiments. First, we fix the pinning locations (q_1, q_1/q_2 and $q_1/q_2/q_3$) and set the pinning potential to be equal to $2000J/m^3$ [17]. This condition is set to simulate the intentional pinning and depinning to study its impact on shift current. Next, we distribute the pinning potential to two and three equal and smaller pinning sites to simulate the impact of unintentional notches due to process variations.

For simulation we assume a NW length of 2um and fix the pinning sites at q_1=0.5um, q_2=1um and q_3=1.5um (Fig. 2(a)). The pinning width (d) is assumed to be 150nm. Fig. 2(b) shows the ψ vs. q plot of DW (for pinning site at q_1 and V_{pin}=$2000J/m^3$) for three different magnitudes of injected shift currents. The DW



(a) (b) (c) (d)

Fig. 2. Domain wall pinning: (a) nanowire with pinning sites at q_1, q_2 and q_3. The notch depth and width is d, nt respectively. Modeling of process variation in d, nt is also shown, (b) ψ vs. q plot of DW for pinning at q_1. The DW depins with u=100m/s, (c) ψ vs q of DW for one and two notches with Vpin =2000 J/m^3 and two notches with V_{pin} =1000 J/m^3, (d) plot showing transient velocity for one deep pinning and two cases of shallow pinning. Here α=0.01, β= 0.02 and Δ=25nm is used.

gets pinned in the first two cases (u=80m/s and 90m/s) but dislodges successfully with u=100m/s. This plot indicates the need of higher current (i.e., higher power) to dislodge the DW. Fig. 2(c) and (d) illustrates the results with pinning at two sites (at q_1, q_2, with V_{pin1}= V_{pin2}=2000J/m^3). With u=100m/s the DW gets depinned from q_1 but gets pinned at q_2. This indicates that velocity degradation due to first notch (even though unpinned) can cause pinning in the next notch. The same current successfully dislodges two notches of half the pinning potential (i.e., V_{pin}=1000J/m^3). This is due to the location of pinning sites. If multiple notches are located close to each other they can pin the DW, due to DW velocity degradation by the notches. If the new notch arrives before the full recovery of DW velocity from the previous notch then it becomes prone to get pinned. It can be observed that the average velocity of the DW can be affected significantly due to presence of unintentional variation induced notches.

In order to study the impact of variations we first model the relationship between depinning magnetic field (H_{th}) and its dependency on notch depth (*nt*) for the NW [17,18,20]. Next we study the presence of single notch at q_{pin}=0 under process variation induced notch width (*d*) and depth (*nt*) fluctuations. The variations in *d* and *nt* is assumed to be Gaussian with mean (μ) and sigma (σ) of (μ_d, σ_d) = (0, 6.66nm) and (μ_{nt}, σ_{nt}) = (0, 50nm). Supply voltage of the shift circuit is swept from 0 to 3V and minimum voltage to dislodge the DW is plotted in Fig. 3(a) for 1000 runs of Monte Carlo simulation. The unwanted pinning of DW is dominated by the long tail of the distribution which indicates that random process variations can have a considerable impact on the velocity of DW.

C. *Relationship between DW Pinning and PUF*

Pinning of DW creates randomness in the DW velocity that can be exploited to generate authentication key. The basic premise is to trigger a DW race between NWs in the array. Due to variation in speed the DWs will reach the read head at different times. If the read timing edge is fixed, some NWs will read 0 and the others will read 1 at the end of shift and read operation. This random pattern in the DWM is used as the signature (memory-PUF). Process variations being random and unique to every IC, the key generated will vary die-to-die. The pattern generated through DW race is unclonable because of its dependence on inherent process. The similar principle can also be used to create a relay-PUF.

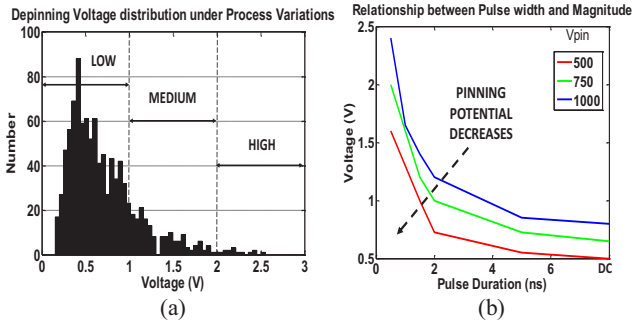
Fig. 3(b) shows the dependency of shift voltage pulse width and pulse magnitude to dislodge the DW from three different pinning potentials. It is interesting to observe that a wider pulse can depin the DW with smaller magnitude of pulse. However as the pulse width becomes narrower, the magnitude of pulse needed to depin goes up. For the sake of clarity, pulse magnitude for DC input condition is also shown in x-axis. Note that there are two conditions, voltage magnitude and pulse width that directly affect the DW velocity. This provides us two extra knobs (challenge) to manipulate the DW motion, thus, enabling us to use these two factors as challenges for our DWM-PUF.

III. DMW-PUF

In the previous section we introduced the basics of DW and the effects of intentional and variation induced pinning. In this section, we explain the circuit details to design two flavors of PUFs namely relay-PUF and memory-PUF.

A. *DWM Relay-PUF*

This is similar to an arbiter based PUF, where we combine multiple dual NW stages with a muxing circuit in between each stage to toggle paths (Fig. 4). The DWs are first nucleated in all the NWs, and are raced against each other by the application of shift current. The switching circuitry is used to toggle between paths in accordance to a challenge pattern (select signal). An arbiter block is placed at the end to compare the arrival times of the respective DWs. More the number of stages, higher is the degree of randomness in the signature. In the following



(a) (b)

Fig. 3. (a) Distribution of depinning voltage under process variation and, (b) dependence of shift pulse magnitude on pulse duration for different amount of pinning potentials.

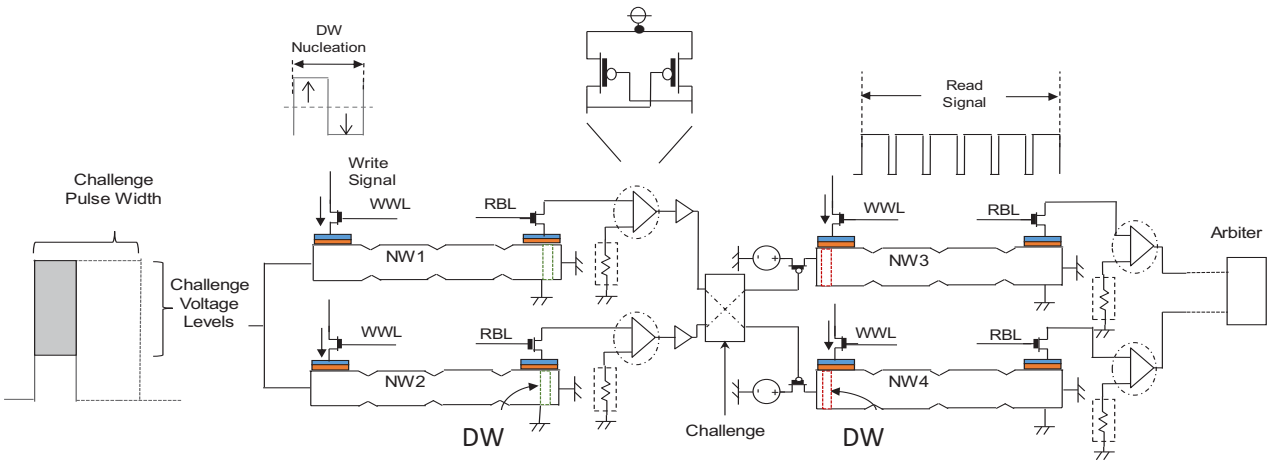


Fig. 4. Overview of the relay-PUF comprising of multiple stages of parallel NWs, write and read heads, sensing circuitry, switching block and an arbiter.

paragraphs, we provide a detailed explanation of the DWM relay-PUF.

Challenge: In contrast to conventional delay-PUF where only muxing is used as challenge, the relay-PUF also provides two additional sets of challenges namely shift pulse magnitude (PM) and pulse width (PW). These new challenges can be employed to increase the size of challenge- response pairs with low area overhead. This is mainly due to the fact that less number of stages can generate large set of challenge-response pairs by mixing different challenges.

DW nucleation and relay race: Each NW has fixed dimension. In order to obtain adequate amount of randomness, a long chain of such NWs are used. First the DWs are nucleated in all the NWs by applying a pulsed (+ & -) current and activating the write word line (wWL). Next, the shift signal of stage-1 is activated that triggers the DW race in two parallel paths. The read head is activated by pulsing the read word line (rWL). As soon as the resistance sensed by the read head changes, the shifting of the current stage is stopped and the shift signal of the following stage is fired. Hence the DW race is relayed to the next stage. This is identical to signal propagation in delay-PUF. The mux select determines whether the upper or lower DW will be fired in the following stage. The sequence of events is illustrated in Fig. 5.

Response: The response of the relay-PUF is determined by an arbiter that decides the early arrival of DWs in parallel NWs. If the top (bottom) DW reaches first the response of the PUF is 0 (1). The NW-NW variation of size and location of surface roughness affect the DW velocity increasing the randomness of the outcome of the race. Depending on the path, a fast DW in one NW can travel through a NW with higher surface roughness slowing down its speed. On the contrary the slow DW can travel through a smoother NW in the following stage increasing its speed. The response is also dependent on shift pulse challenges. Higher pulse width and magnitude will change the speed of DW and will increase the randomness in response.

Simulation Results: First we demonstrate the relay race between two DWs due to process variations. For this simulation we assume two parallel NWs each containing two stages. The length of each NW is 2um and the process variation is modeled by assuming three pinning notches at 0.5um, 1um and 1.5um along the length of the NW. The values of pinning potentials are assumed to be 1000, 750 and 500 J/m^3 for the top NW and 500, 750 and 1000 J/m^3 for the bottom NW. Fig. 6(a) shows the DW position in two NWs *w.r.t* time. It can be observed that DWs race at different speeds due to difference in pinning potentials. The DW in the bottom NW (i.e., NW2) arrives earlier than the top NW (i.e., NW1). The relay of the DWs from one stage to another through the challenge mux is shown in Fig. 6(b). NW1 finishes the race and the sense amplifier triggers the shifting of DW in NW3. At the end of race in second stage NW4 finishes much earlier that NW3 due to cumulative relay effect.

Fig.6(c) shows the read head functionality. The sense amplifier is designed to output a default high value. When the DW arrives the output is toggled to low. It can be observed that RL2 toggles before RL1 indicating early arrival of DW2. The next stage outputs RL3 and RL4 that toggle at the end of the race. Signal RL4 transitions to a low value much before RL3 winning the race. It must be noted that, the behavior of this PUF can be altered by changing the challenge. For the detailed simulation, we extend the relay-PUF to a 2 parallel path, 6 stage design. The total number of challenges in this PUF is 2^5 i.e., 32. Therefore 32 different path combinations are possible, which can trigger

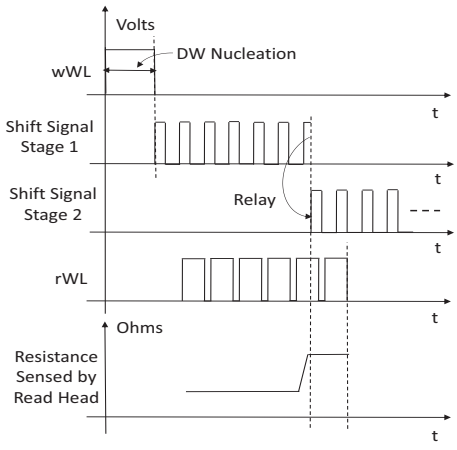
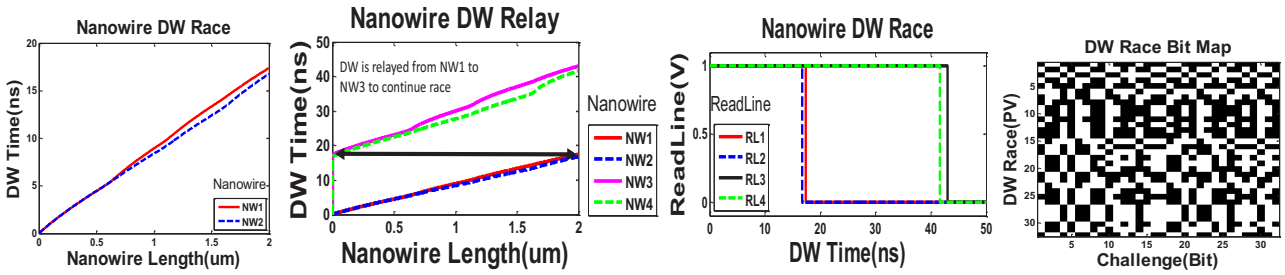


Fig. 5. Timing diagram representing the wWL, the shift signals for each stage, the rWL and the variation of resistance sensed by the read head.



(a) (b) (c) (d)

Fig. 6. (a) Shows the NW race between 2 NWs (NW1 & NW2), (b) the DW information being relayed to the next NW stage (NW3 & NW4), (c) shows the sense amplifier output at the end of DW arrival at each stage. This is signal is active low and triggers the race in the following stages and, (d) response of 6-stage relay-PUF for 32 challenges for 32 different dies.

the race by producing a one bit response. As described in Section II, process variation within each NW can result in different pinning potentials for each notch. For this simulation the pinning locations in the NW is kept same as before. However the mean pinning potential is assumed to be 500J/m^3 and a variation of 150 J/m^3 (3 sigma) is added to model, to incorporate the effect of process variation-induced pinning potentials. The relay-PUF's responses for all 32 possible challenges are simulated. Next, new sets of process variations are applied to the PUF to simulate inter-die responses.

Fig. 6(d) shows the PUF response obtained from 32 different dies (y-axis) and 32 challenges (x-axis). It can be seen in the bit map that process variation within the nanowires can cause the arbiter outputs to change. The challenge also triggers a change in the PUF response. The average die-to-die Hamming Distance (HD) is found to be 47%.

B. *Memory-PUF*

This PUF is similar to SRAM based PUF where the entire memory bank is potentially used to obtain the authentication key unique to the chip at hand. The DWs in all NWs in the memory banks are fired simultaneously. The race concludes when the read signal is asserted. The DWs winning the race are set to 1 whereas the others are set to 0. In contrast to relay-PUF, this design does not require any circuit overhead. Due to non-volatile nature of the bitcell this PUF is also low-power.

Challenge: In contrast to SRAM-PUF where the memory pattern is solely dependent on power up and variations, the DWM memory-PUF depends on both variations and shift pulse characteristics (magnitude and width). The challenges are the address of the array and shift pulse.

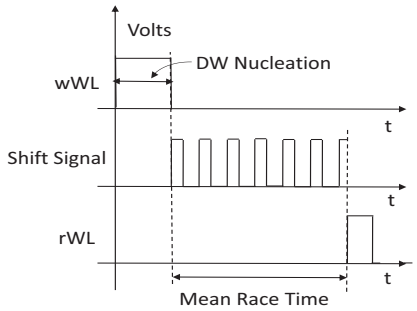


Fig.7. Timing diagram representing the wWL, the shift signal and the rWL.

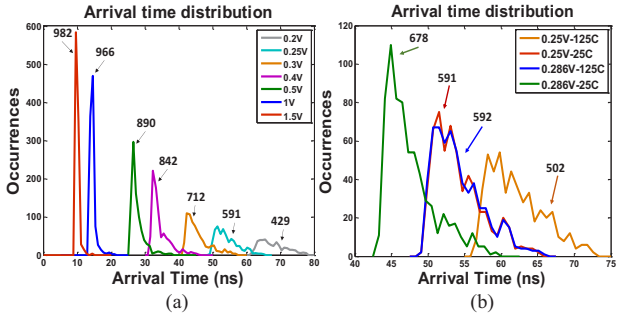
DW nucleation and race: Similar to relay-PUF, first a single DW is nucleated in all NWs present in the array (Fig. 7). Next, the DWs are shifted/raced by a shift pulse challenge. The rWL is fired after a conservative time to screen the pinned DWs at the end of the race for determining the outcome.

Response: The response of this PUF is the output of the array when a certain address is accessed for a particular pulse setting. The value of the bitcell is '1' ('0') if a high (low) resistance is read from the read head as discussed before.

Simulation Results: For this PUF flavor, we consider 100x100 array of DWM. The intra-die variation is modeled by varying the pinning depth and width as Gaussian distribution with (μ_d, σ_d) to be (0, 5nm) and (μ_{nt}, σ_{nt}) to be (0, 2nm). Three notches are assumed per NW at 0.5um, 1um, 1.5um. The pinning potentials are determined from the notch dimensions.

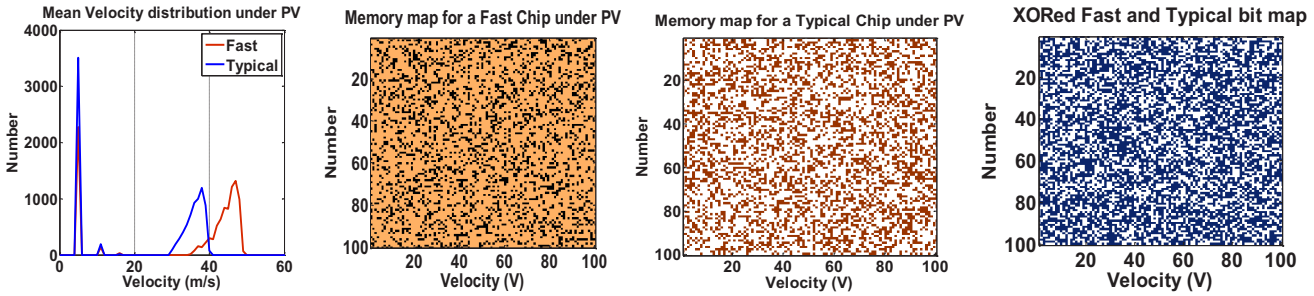
The simulation at 1V shift pulse shows that only 34 out of 1000 NWs get the DWs pinned (Fig. 8(a)). Considering the fact that the pinned DWs will result in a '0' response, this race condition will produce uneven '1's and '0's. In order to balance the '0' and '1' we reduce the shift pulse voltage, and note that shifting at 0.25V roughly produces 59% of '1' (i.e., the DWs that win the race). By operating the memory-PUF at this voltage, there is no need to correctly manage the reference read time as the DWs that get pinned will always loose the race. The problem with this method is its susceptibility to variations in temperature. The NWs resistance is directly proportional to the increase in temperature [17]. This impacts the amount of shift current and affects the DW velocity.

Fig. 8(b) shows the DW arrival time distribution at 0.25V for two temperatures 25C and 125C. It can be observed that high temperature pins more DWs (409 vs 498) and changes the signature of memory-PUF. To maintain the PUF robustness we propose shift voltage boost at high temperature to negate the



(a) (b)

Fig. 8. Arrival time distribution for (a) different shift voltage settings at 25C and, (b) two voltages settings at 25C and 125C. The successful NWs and the total number are also shown for 1000 runs of Monte Carlo.



(a) (b) (c) (d)

Fig. 9. (a) Velocity distribution in the memory array for fast and typical corners. A memory array bitmap comprising of 100X100 bits showing, (b) fast corner, (c) typical corner and, (d) differences in the signature between fast and typical die.

effect of extra DWs pinning. Our simulation indicates that boosting by 36.2mV brings back the number of pinned DWs back to 408 at 125C.

To analyze the die-to-die uniqueness in response we model the inter-die process corners (fast and typical) by skewing the NW width and thickness by a factor of 10% i.e. fast corner is (-10%, -10%). Fig. 9(a) shows the distribution of velocity for typical and fast corners. Again the reference is selected to screen the pinned DWs for the two corners. Fig. 9(b) shows the 0/1 pattern obtained for a fast NW. This pattern or signature is the device identity which varies from die-to-die. We compare the bit pattern for the fast corner with the typical die. Fig. 9(c) shows the bitmap pattern for a typical NW and, Fig. 9(d) shows the XORed pattern for fast-typical case. It is evident that the signature differs from one another and ~44% Hamming distance is achieved.

So far we have only described a NW with one read and one write head. However, it is possible to have multiple read heads on a NW, which are individually selected by a wordline (WL). This enables the use of the head selection as another challenge tier. Applying this to our memory PUF based design, we can achieve a larger number of responses for the same size array or maintain the number of responses and reduce the size of the memory array. It is important to note that the selection of heads must be done in an orderly fashion (i.e. head1-head2-head3…) to avoid the need to reset the DWs before every analysis. Additionally, since the shift power is dependent on the length of the NW, the use of multiple heads in the NW (Fig. 10) will dramatically reduce the power consumed. By increasing the number of heads, a power reduction of ~10X over SRAM can be achieved for the same number of challenge response pairs.

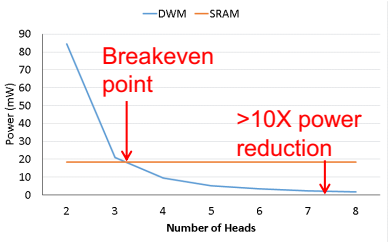


Fig. 10. Power vs # of heads for DW memory-PUF. More than 10X power saving is possible compared to conventional SRAM-PUF

IV. CONCLUSIONS

We presented the application of spintronics for hardware security and authentication. Two novel spintronic PUFs were described namely; relay-PUF and memory-PUF. Both PUFs exploit the process variation induced DW pinning and slowdown to generate the response. The proposed designs provide additional knobs e.g., shift pulse, number of access ports to expand the set of challenge-response pairs. Due to non-volatile nature of the structure, the proposed memory PUF is low-power compared to SRAM PUF.

V. ACKNOWLEDGEMENTS

This paper is based on work supported by Semiconductor Research Corporation (#2442.001).

VI. REFERENCES

[1] B. Gassend et al. “Identification and Authentication of Integrated Circuits” Concurrency and Computation: Practice and Experience, 2004.
[2] J. W. Lee et al. “A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Application,” VLSIC, 2004
[3] B. Gassend et al. “Physical Random Functions,” M.S. thesis, Massachusetts Institute of Technology (MIT), 2003.
[4] B. Gassend, et al. “Silicon Physical Random Functions,” CCS, 2002.
[5] J. Guajardo, et al. “FPGA Intrinsic PUFs and Their Use for IP Protection,” CHES, 2007.
[6] S. Garrett et al., "Nanoelectronics and Hardware Security." NSC, 2014.
[7] S. Garrett et al., "Foundations of memristor based PUF architectures." NANOARCH, 2013.
[8] S. Garrett et al.,"Hardware security strategies exploiting nanoelectronic circuits." ASP-DAC, 2013.
[9] R. Karri et al. "Nano-PPUF: A Memristor-based Security Primitive." ISVLSI, 2012.
[10] J. Rajendran et al. "Nanoelectronic Solutions for Hardware Security." IACR, 2012.
[11] S. Garrett et al. "A write-time based memristive PUF for hardware security applications." ICCAD, 2013.
[12] S. Parkin, et al. "Magnetic domain -wall racetrack memory." Science, 2008.
[13] S. Ghosh, "Path to a TeraByte of on-chip memory for petabit per second bandwidth with< 5watts of power." DAC, 2013.
[14] A. J. Annunziata et al., “Racetrack memory cell array with integrated magnetic tunnel junction readout, IEDM 2011.
[15] M. Kryder et al., “After hard drives—what comes next?”, TMag, 2009.
[16] A. Thiaville, et al. "Domain-Wall Dynamics in Nanowires and Nanostrips." Spin dynamics in confined magnetic structures III, 2006.
[17] M. Hayashi, "Current driven dynamics of magnetic domain walls in permalloy nanowires." PhD diss., Stanford University, 2006.
[18] T. Suzuki, et al. "Analysis of current-driven domain wall motion from pinning sites in nanostrips with perpendicular magnetic anisotropy." JAP, 2008
[19] http://rijndael.ece.vt.edu/puf/background.html
[20] A. Iyengar et. al., “Modeling and analysis of domain wall dynamics for robust and low-power embedded memory”, DAC, 2014.