Spintronic PUFs for Security, Trust, and Authentication

ANIRUDH IYENGAR, SWAROOP GHOSH, KENNETH RAMCLAM, JAE-WON JANG, and CHENG-WEI LIN, University of South Florida

We propose spintronic physically unclonable functions (PUFs) to exploit security-specific properties of domain wall memory (DWM) for security, trust, and authentication. We note that the nonlinear dynamics of domain walls (DWs) in the physical magnetic system is an untapped source of entropy that can be leveraged for hardware security. The spatial and temporal randomness in the physical system is employed in conjunction with microscopic and macroscopic properties such as stochastic DW motion, stochastic pinning/depinning, and serial access to realize novel relay-PUF and memory-PUF designs. The proposed PUFs show promising results (∼50% interdie Hamming distance (HD) and 10% to 20% intradie HD) in terms of randomness, stability, and resistance to attacks. We have investigated noninvasive attacks, such as machine learning and magnetic field attack, and have assessed the PUFs resilience.

CCS Concepts: • **Security and privacy → Hardware-based security protocols**; • **Hardware → Spintronics and magnetic technologies**

Additional Key Words and Phrases: Domain wall memory, nanowire, hardware security, physically unclonable function, chip authentication, threat models, magnetic attack

ACM Reference Format:
Anirudh Iyengar, Swaroop Ghosh, Kenneth Ramclam, Jae-Won Jang, and Cheng-Wei Lin. 2016. Spintronic PUFs for security, trust, and authentication. J. Emerg. Technol. Comput. Syst. 13, 1, Article 4 (April 2016), 15 pages.
DOI: http://dx.doi.org/10.1145/2809781

1. INTRODUCTION

Hardware security, trust, and authentication are inherently intertwined with each other. The untrusted design environment results in infected hardware that in turn brings the need to authenticate the integrated circuits (ICs). Although software-based security solutions are easy to implement, hardware solutions such as hardware encryption, physically unclonable functions (PUFs), true random number generators (TRNGs), and tamper detection sensors have shown great promise to meet power/performance standards, while uncovering and solving emerging security issues, such as Trojan insertion, IC recycling, and side-channel attacks [Abramovici et al. 2009; Rostami et al. 2013]. The security primitives typically extract the spatial and temporal randomness and inherent entropy present in the system using carefully designed harvesting circuits for generating unique identification keys. The downside of complementary metal-oxide semiconductor (CMOS)-based circuits is area and power overhead, sensitivity to environmental fluctuations, limited randomness, and

This article is based on work supported by Semiconductor Research Corporation (#2442.001) and National Science Foundation (CNS-1441757).
Authors' addresses: A. Iyengar, S. Ghosh, K. Ramclam, J.-W. Jang, and C.-W. Lin, Computer Science & Engineering, University of South Florida, 4202 E. Fowler Avenue ENB 118, Tampa, FL 33620-5399, U.S.A; emails: {anirudh, swaroopghosh, kramclam, jjang3, chengwei}@mail.usf.edu.

DOI: http://dx.doi.org/10.1145/2809781

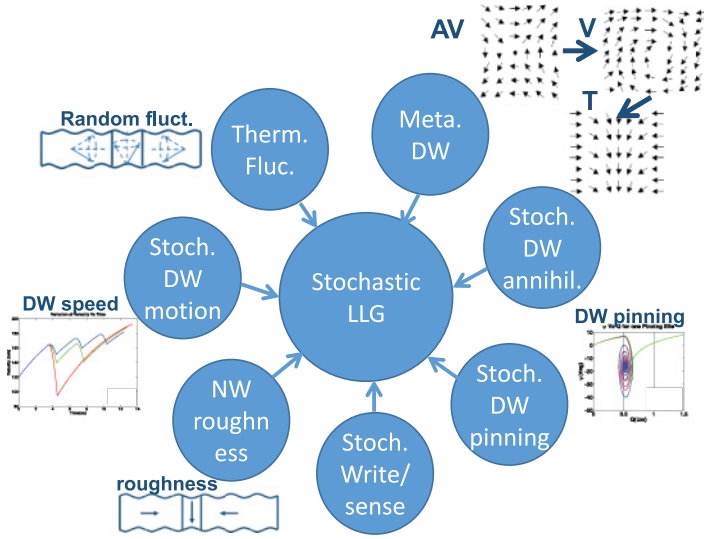


Fig. 1. Sources of entropy and randomness in DWM system.

entropy offered by the Silicon substrate. This brings the need to exploit emerging technologies containing an abundance of entropy and physical randomness while being robust, energy-efficient, and fast. We note that spintronics [Žutić et al. 2004; Bandyopadhyay et al. 2008; Wolf et al. 2001] is one such possible candidate that possesses an untapped source of entropy in the system besides having an energy-efficiency of higher order of magnitude than CMOS. Some examples are shown in Figure 1.

The experimental results on spin valves, magnetic-tunnel junctions (MTJ), domain wall magnets (DWM), and so on, by Nikonov et al. [2006], Driskill-Smith [2010], Parkin et al. [2008], Berger et al. [1984], Freitas et al. [1985], Hayashi et al. [2006], Wang et al. [1999], Zhang et al. [2004], Thiaville et al. [2006], Duine et al. [2007], Hermann et al. [2013], Okuno [1997], Alekseev et al. [1992], Edwards et al. [2002], and Jamali et al. [2012] 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 the 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. The thermally activated electrons in the material add to the entropy. Besides, the magnet is also sensitive to physical randomness. One such magnetic system with abundance of entropy is DW in permalloy nanowire (NW) with 20% Fe and 80% Ni (Fe20Ni80). We propose methodologies to harvest the entropy to realize hardware security primitives, such as PUF. Design of PUF using memristors have been proposed in the past [Rose et al. 2014; Rajendran et al. 2012]. However, due to the emerging nature of spintronics and hardware security, very little research [Iyengar et al. 2014; Iyengar et al. 2015; Tanamoto et al. 2011] has been done to bridge the two fields. Although a practical demonstration of a DWM-based PUF is still missing, works illustrating DWM for cache [Annunziata et al. 2011], content addressable memory [Nebashi et al. 2011], and highly efficient DW motion [Parkin et al. 2008; Yang et al. 2015] have been previously described, which show promise.

Although DWM is a promising memory technology, it brings in an important security concern. It is susceptible to contactless tampering efforts, for example, by subjecting it to strong external magnetic fields, an adversary can corrupt stored contents. The

fixed layer of the MTJ is robust. However, the free layer could be toggled through both spin polarized current as well as magnetic field, making them vulnerable toward tampering. The ease of tampering the data underscores the need of quantifying the impact of magnetic attack and exploring effective, low-overhead protection mechanisms [Samsung 2013].

The key contribution of this article is that it provides a transformative application of spintronics by (a) engineering new techniques to harvest the randomness in magnetic NW; (b) combining the circuits and models of nonlinear magnetic dynamics to realize hardware security primitives such as PUF; (c) validating the models and design ideas under harsh conditions; and (d) attack scenarios, such as magnetic field and machine learning. Due to superior energy-efficiency and the footprint of DWM, the proposed circuits are orders of magnitude lower in power and density, as compared to its CMOS counterparts. Due to the nonlinear dynamics of the magnetic system, the quality of spintronic security primitives is superior. Metrics such as entropy, uniqueness, repeatability, number of trials, robustness, power consumption, and attack resilience are employed to quantify the strength of proposed security primitives.

The article is organized as follows. Section 2 describes the prior research, novelty, and approach. Two flavors of PUF architectures, namely relay-PUF and memory-PUF, are introduced in Section 3. Simulation results demonstrating various quality metrics, power dissipation, and area overhead are presented in Section 4. The attack scenarios and the resilience of the proposed DWM-PUFs compared to CMOS-PUFs are described in Section 5. Conclusions are drawn in Section 6.

2. RELATION TO PRIOR WORK, NOVELTY, AND APPROACH

2.1. Prior Work

Extensive research has been conducted to address hardware security, trust, and authentication mechanisms. To deter IC cloning and stealing of secure keys, PUF [Pappu 2001] has been proposed. PUF generates the response (key) to a particular challenge from physical properties of the chip. Several flavors of PUFs, for example, optical PUF [Tuyls et al. 2006], delay PUF [Maiti et al. 2010], static random access memory (SRAM) PUF [Holcomb et al. 2009], flash PUF [Wang et al. 2012], and flip-flop PUF [Zheng et al. 2013] have been introduced. The common limitations of CMOS-PUF designs are area/power overhead, restricted number of challenge-response sets, robustness to environmental fluctuations, and most importantly, limited physical randomness in the system. Specially crafted circuit structures such as SRAM and flip-flop are used to amplify the effect of physical randomness. Nano-electronic PUFs [Rose et al. 2014; Rajendran et al. 2012] using memristors have been presented to leverage properties like initialization, nonvolatility, density, resistance states, etc., to address some of the challenges faced by CMOS PUFs.

2.2. Novelty

Spintronics have been extensively studied for logic and memory applications due to its superior energy-efficiency and nonvolatility [Wolf et al. 2001]. However, to the best of our knowledge, a detailed study of spintronic randomness and other micro- and macroscopic properties have not been attempted before for hardware security, trust, and authentication. For the first time, we proposed a technique to exploit the roughness of NW, the resulting nonlinear DW dynamics, and stochastic DW pinning for hardware security. The proposed approach ranges from the modeling of spintronic devices and security specific properties to security circuit design and analysis. The following paragraphs provide further details on the novelty of the proposed work.

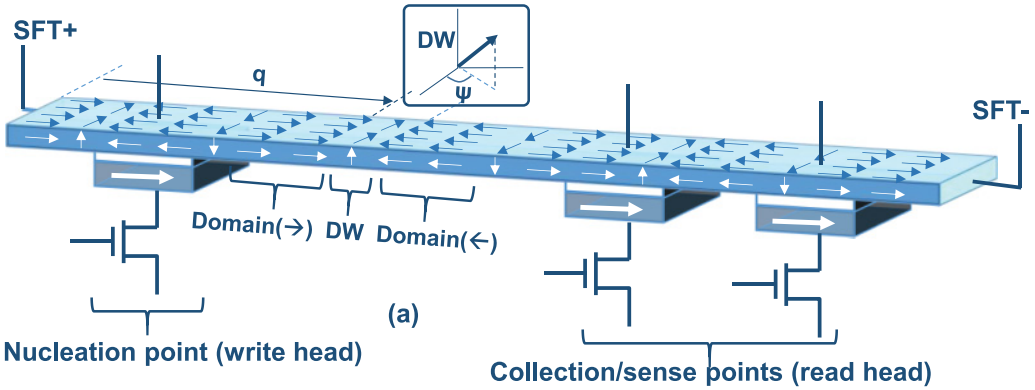


Fig. 2. Schematic of DWM with write/read heads for nucleation/sensing and shift contacts for moving the DW along the NW.

2.3. Approach

The first aim is to capture the nonlinear dynamics of DW in detailed physics-based models. This is accomplished by modeling the process variations in the DW NW. The Landau-Liftshitz-Gilbert (LLG) equation to solve the DW dynamics is modified to incorporate the effect of process variations. Harvesting technique is designed to capture the noise and randomness with minimal disturbance to the underlying system and convert them into measurable quantities. Next, the harvesting circuit is employed as the building block for the PUF design. The quality of the PUF, for example, entropy, uniqueness, repeatability, robustness, and resiliency toward attacks, is ensured by detailed analysis. Finally, the proposed spintronic PUFs are benchmarked against conventional CMOS-PUF architectures. The detailed approach is outlined below.

DWM:

Figure 2 shows the schematic of DWMs. The formation of DWs takes place at the interface of two distinct magnetic polarities, or domains. The magnetization reversal of the domain is essentially controlled by DWs. The key mechanism is the exchange interaction between itinerant electrons with the local magnetization and the resulting transfer of spin-torque to push the DWs. DWM is a dynamical system and the magnetization dynamics is governed by the LLG equation [Zhang et al. 2004; Thiaville et al. 2006]

$$\frac{\partial \vec{m}}{\partial t} = \underbrace{-\gamma\, \vec{m} \times H_{eff}}_{precession} + \underbrace{\alpha\, \vec{m} \times \frac{\partial \vec{m}}{\partial t}}_{damping} - \underbrace{u(\vec{j}\,.\nabla)\vec{m}}_{adiabatic} + \underbrace{\beta u\, \vec{m} \times (\vec{j}\,.\nabla)\vec{m}}_{non-adiabatic}, \tag{1}$$

where $\vec{m}$ and $\vec{j}$ are unit vectors representing local magnetic moments and current flow. α and β represent the Gilbert's damping parameter and the nonadiabatic spin transfer term, respectively. The effective field is represented by $H_{eff} = -\frac{1}{\mu_0 M_s}\frac{\delta w}{\delta \vec{m}}$. The spin transfer torque parameter "u" is proportional to the current density J, the spin polarization P. It is given by $u = \frac{\mu_B JP}{eM_s}$, where M_s is the saturation magnetization, w is the energy density, and μ_B is the Bohr magnetron. It must be noted that the above equation does not take into account the stochastic variation introduced into the system, due to thermal and voltage fluctuations.

The LLG equation is modeled in verilog A. It is worth mentioning that access devices (essentially MTJs, Figure 2) are typically added to inject currents (for nucleating DW)

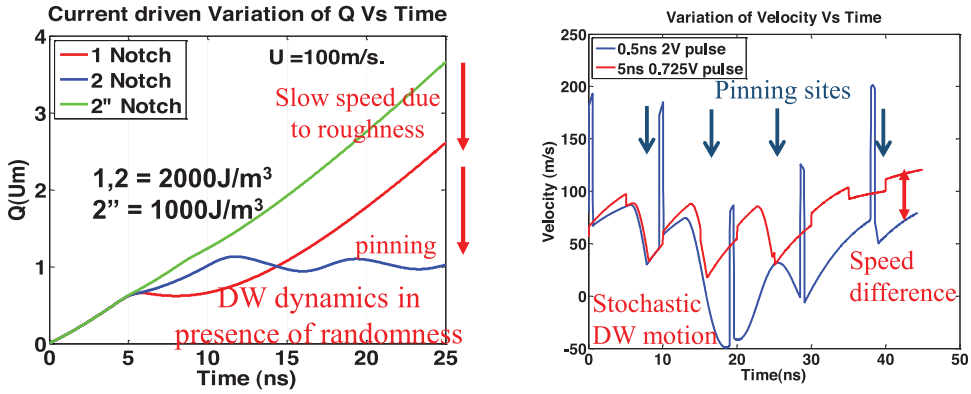


Fig. 3. (a) DW dynamics in presence of physical roughness induced slowdown and eventual pinning. Stochastic motion of DW. A misaligned shift pulse reduces velocity, and (b) DW dynamics with two different shift current magnitudes and duty cycles, but same average value is also shown.

and collect the DW dynamics (i.e., sensing the magnetization of domains). Shift contacts are added to inject current and push the DWs along the NW.

Entropy and Randomness in DWM:
The interaction between the conduction electron of injected current, thermally activated electrons, and local magnetization is a source of entropy [Duine et al. 2007; Hermann et al. 2013; Okuno 1997; Alekseev et al. 1992; Edwards et al. 2002; Jamali et al. 2012] (Figure 1). In this work, we incorporate the randomness in physical parameters in the model. In NW, the roughness is modeled as triangular notches with width (d) and depth (t). The pinning energy is given as follows [Hayashi 2006]:

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

where q_{pin} is the pinning site, V_{pin} is the pinning potential at that particular location, and q is spatial location on the NW. By determining an accurate relation between V_{pin} and t, and assuming Gaussian distribution of d and t, we can obtain the statistical nature of DW dynamics in the nonuniform NW. Figure 3 illustrates the initial results, showing DW motion by using a curve-fitting model of V_{pin}. It can be observed that the DW dynamics are nonlinear in nature, which makes them resistant to modeling-type attacks.

Microscopic Properties:
Besides entropy, the DWM possesses several microscopic properties (discussed below) that are modeled in our simulation framework:

(i) *Stochastic DW motion (speed and polarity)*: The DW speed depends on the type of wall, spatial location of notches (which is stochastic in space), shift current magnitude, and frequency, as well as duration for which pulse is applied. The phase between a notch and pulse arrival time is a stochastic process in time domain. Figure 3 represents the stochastic nature of notch location with respect to shift pulse. The DW with the same initial velocity simulated with two different shift pulse characteristics (with same average value) moves with different velocities. Therefore, DW velocity is stochastic and our model will capture the behaviors for random roughness of the NW and DW nucleation.

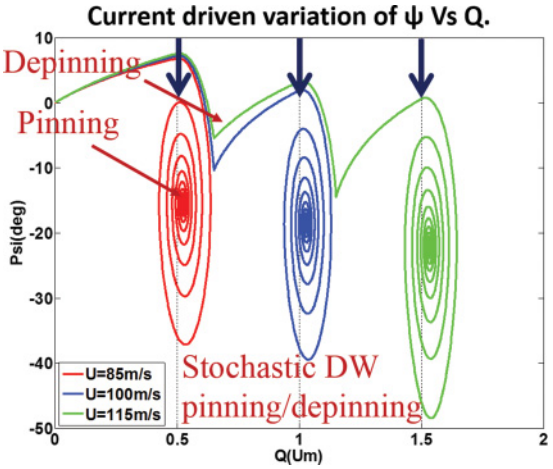


Fig. 4. Stochastic pinning of DWs with respect to three different shift currents.

(ii) *Stochastic DW pinning:* The DW moves smoothly if the NW is free of roughness (notches). However, process variation-induced edge roughness can hinder and slow down the DW that may result in eventual pinning. Pinning of the DW is a stochastic process and depends on surface roughness (magnitude and spatial location), injected shift current, and magnetization dynamics. Once pinned, the DW behaves as a particle trapped in a potential well. The depinning is also a stochastic process and depends on the injected current magnitude, frequency, and environmental conditions. Figure 4 represents the stochastic nature pinning due to notch location, DW speed, and shift pulse. Figure 4 shows that an out-of-sync pulse may degrade the DW speed and lead to pinning.

Macroscopic Properties:

(i) *Initialization and resetting:* Initially, the NW is magnetized in a preferred direction determined by the balance of exchange and anisotropy energies. Therefore, the NW is free of DWs before first access. In order to populate new information in the NW, DWs are nucleated using access MTJ (write head) by injecting sufficient current in the orthogonal direction to flip the local magnetization under the MTJ. The NW can be flushed out by simply injecting current through shift contacts and moving the bits out.

(ii) *Bipolar DW nucleation:* The nucleation of DW in the NW is bipolar in nature. The current polarity (through write MTJ) determines the type of DW (head-to-head or tail-to-tail).

(iii) *Multiple domains/NW:* The NW can hold multiple domains or information bits by nucleating new DWs through write MTJ and shifting them in the NW similar to shift register. The limit of bits per NW is set by the NW dimensions.

(iv) *Serial access and bipolar shifting:* In contrast to conventional magnetic devices, DWM stores multiple bits of information. The group of DWs is shifted together by injecting current. The bits in the NW can be shifted in both directions by changing the current polarity.

(v) *Miscellaneous properties:* DWM provides opportunity to exploit multiple sense points (read heads) along the NW for continuous collection of entropy and randomness. The position of read heads are determined according to requirements and modeled accordingly. Each DWM is also characterized in terms of power

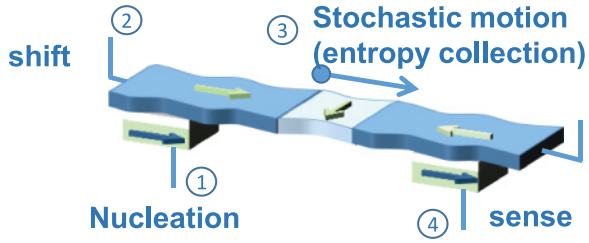


Fig. 5. Harvesting entropy and randomness through DW nucleation (1), shift (2), DW motion (3), and sense (4).

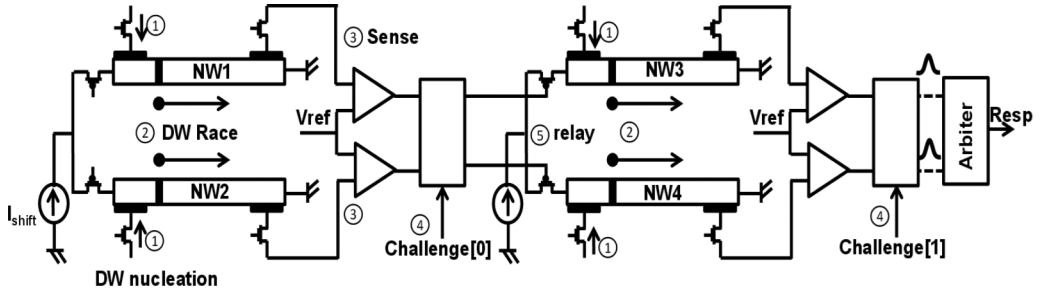


Fig. 6. Schematic of DW relay-PUF. Ishift pulse magnitude and width can also be used as challenges. Sequence of events is numbered from 1 to 5.

and performance for DW nucleation, shift, and sense operations. The physical dimension of the DWM with integrated MTJ access devices is estimated for footprint analysis.

3. PUF ARCHITECTURES

In this section, we propose a simple technique to harvest randomness. This is followed by two flavors of PUF architecture, namely relay-PUF and memory-PUF.

3.1. Harvesting Entropy and Randomness

The objective of harvesting techniques is to convert the entropy to measureable quantities, like voltage, current, and resistance, without disturbing the stochastic process by employing accurate sense methodology. Figure 5 illustrates an example where a DW is nucleated and moved in the NW by injecting shift current. The DW arrival time under the sense MTJ contains several sources of entropy, namely, metastability of DW, stochastic motion, and stochastic pinning/speed degradation.

3.2. Relay-PUF Design

We harvest the physical randomness in the DWM to generate challenge and response. Figure 6 illustrates a relay-PUF design with series connected NW stages. The conventional muxing circuit between each stage is introduced to toggle paths and creates new challenges. More stages also provide a higher degree of randomness in signature. An arbiter block is placed at the end to compare the arrival times of the respective DWs. The operation of relay-PUF has three stages.

(i) *Challenge:* In contrast to conventional delay-PUF, the relay-PUF also provides extra degrees of freedom to choose challenges, namely, shift pulse voltage, pulse width, and pulse frequency. These new challenges can be employed to increase the number of challenges with low area overhead. Figure 6 shows that obtaining the same number of challenges will require significant area and power overhead.

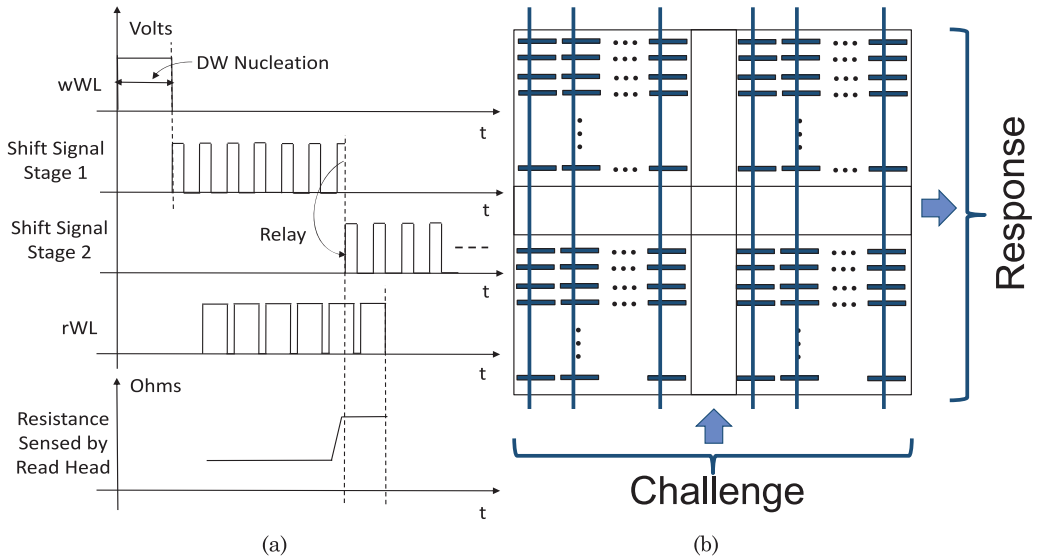


Fig. 7. (a) Timing diagram showing the write and read wordlines and the shift signals for each stage, and the resistance sensed with respect to time; and, (b) schematic of memory-PUF.

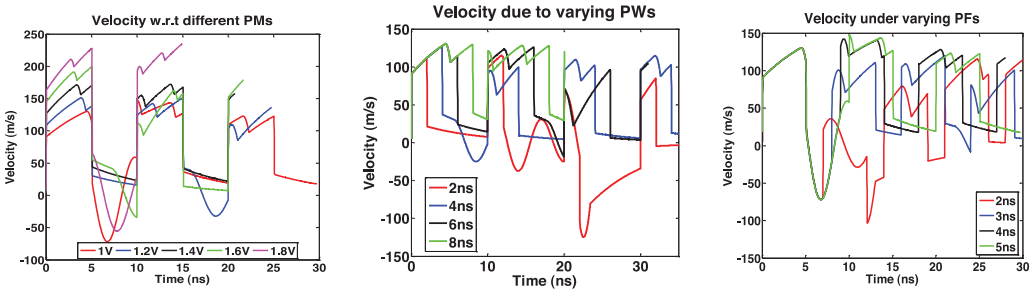
With 1e19 challenges, it will take approximately 10 years to decode the response by an adversary, making the PUF attack-resistant.

(ii) *DW nucleation and relay race:* The first step of operation is to nucleate the DWs in all the NWs by applying a pulsed (+/–) current, during which the write word line (wWL) is activated, as illustrated in Figure 5(a). Next, the shift signal of stage 1 is activated, which triggers the DW race. The read head is activated by pulsing the read word line (rWL). As soon as the resistance sensed by the read head changes (by sensing the magnetization change), the shifting of the stage is stopped. Unlike an inverter chain where the transition propagates from one stage to another, the DW vanishes once it reaches the end of the NW. To enable seamless propagation of the DW, in anticipation of the arrival of the DW after the nucleation stage, the read head is kept asserted to sense the arrival of the DW. Once the read head detects the arrival of the DW (the DW reaches the end of the NW), the shift signal of the following stage is fired, thus relaying the DW information to the next stage. The mux select determines whether the upper or lower DW will be fired in the following stage.

(iii) *Response:* The response of the relay-PUF (0 or 1) is determined by an arbiter that decides the early arrival of DWs in parallel NWs. The switching of paths, in association with shift pulse width, duration, and frequency, provides several layers of randomness in the race condition. As the physical roughness varies NW-to-NW, the DWs will race with different speeds and the response will vary between chips.

3.3. Memory-PUF Design

In addition to the relay-PUF, we also explore memory-PUF, where the entire memory bank is used to obtain the authentication key. A race is employed to characterize the state of each NW in the array. The DWs winning the race are set to 1, whereas the others are set to 0. The random roughness in NWs would be mapped to random initialization of the array. Due to zero standby leakage of the bitcell, this PUF is low power compared to SRAM PUF. The schematic of memory-PUF is shown in Figure 7(b).



(a) (b) (c)

Fig. 8. Relationship of DW velocity on the three pulsed voltage conditions (a) for various (pulse magnitude) PMs, (b) for different (pulse width) PWs, and (c) for different (pulse frequencies) PFs (legend shows the off-on time = 5ns, pulse period for (a) and (b) is 10ns).

4. SIMULATION RESULTS

In this section, we present the simulation results and analysis of the proposed PUFs in terms of quality metrics (such as strength, stability, and randomness), area, and energy.

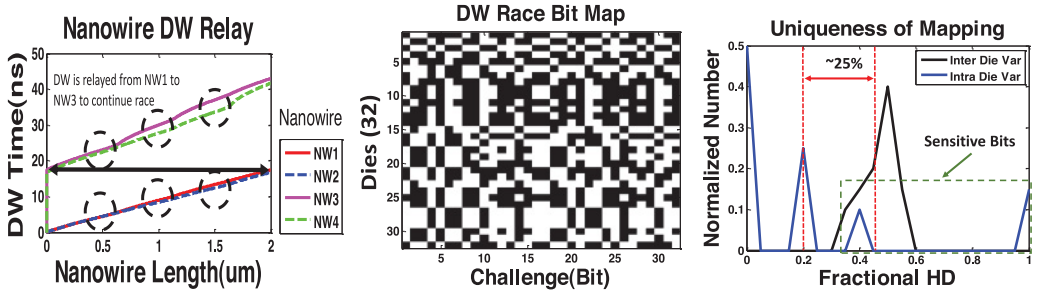
4.1. PUF Strength

The proposed PUFs not only employ the conventional challenges, such as mux switching (for relay-PUF) and row address (for memory-PUF), but also shift current pulse magnitude, pulse width, and pulse frequency as an additional set of challenges. Therefore, the relay-PUF could be categorized as a strong PUF, whereas the memory-PUF could be categorized as a moderately strong PUF. The outcome of the race is highly randomized, as the process variation varies from NW-to-NW and the location of notches are random, both spatially and temporally. The behavior of the DW in response to shift current pulse magnitude, width, and frequency is illustrated in Figures 8(a) and (c). It is evident that DW velocity is strongly dependent on the pulse characteristics. Therefore, shift pulse could also be employed as a challenge. The nonlinear dynamics of the DW also make the proposed PUFs modeling and machine learning attack resilient.

4.2. PUF Randomness and Stability

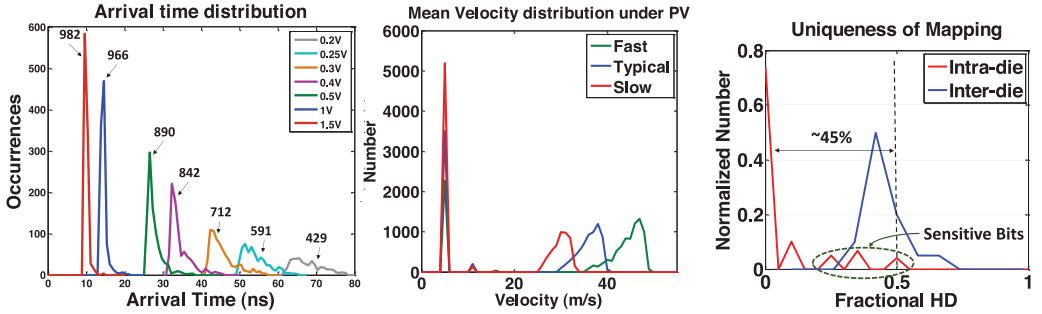
The PUF randomness is measured by the interdie Hamming distance (HD), whereas the stability is measured by intradie HD. First, we present the results for relay-PUF. This is followed by memory-PUF results.

Relay-PUF:
For simulation, we considered six stages. Each NW is 2um long and the surface roughness is modeled by assuming Gaussian pinning potentials (μpin = 500J/m^3, σpin = 50J/m3). For simulation, 25°C and 0.25V is used. The number and location of pinning on the NW is fixed (0.5μm, 1μm, and 1.5μm, respectively). The DW dynamics in the NW are solved by using stochastic 1D-LLG. Figure 9(a) shows the DW race in two NWs with respect to time. The DW in NW2 arrives earlier and conveys the relay to NW4, which wins the race. Note that the behavior of this PUF can be altered by changing the challenge. Figure 9(b) is the PUF response from 32 different dies (y-axis) and 32 challenges (x-axis). The die-to-die average HD is found to be 45%. For intradie HD, we compare the PUF response by considering two extreme operating temperatures, −10°C and 90°C, and voltage variations of ±10%. A total number of 20 chips, each having 100 PUFs, is considered for this analysis. We note a long tail in the distribution is obtained due to sensitive bits that are highly susceptible toward temperature and voltage variations (as seen in Figure 9(c)). In order to ensure low intra-die variation, additional



(a) (b) (c)

Fig. 9. (a) Simulation showing relay race and winning DW, (b) PUF response under variations, and (c) inter- and intradie HD distribution for relay-PUF.



(a) (b) (c)

Fig. 10. Arrival time distribution for (a) different shift voltage settings at 25°C, (b) velocity distribution in the memory array for fast, slow, and typical corners, and (c) inter- and intradie HD distribution for memory-PUF.

techniques should be employed. Few ideas include (a) temporal redundancy, where the response of the bit is observed at different time instances and majority response is used as the final output, and (b) error correction circuitry, such as Von-Neuman corrector [Jun et al. 1999] and run-length encoding [Wang et al. 1999] to fix the unstable bits. An average of 25% separation between the interdie and the intradie variation is observed for relay-PUF which shows good randomness and stability.

Memory-PUF:
In this case, we assume a 100×100 array per PUF. For HD analysis, we assume 20 dies each with 20 such PUF blocks. The notch dimensions for the interdie process variations are varied according to a Gaussian distribution, as described before. The operating voltage is determined to ensure an equal distribution of "1" and "0". The simulation at 1V shift pulse shows that only 34 out of 1,000 NWs get the DWs pinned (Figure 10(a)). Considering the fact that the pinned DWs will result in a 0 response, this race condition will produce uneven 1s and 0s. 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, we ensure that half of the DW will always get pinned and will lose the race. Therefore, the requirement of sensing the arrival time could be relaxed and sensing could be performed after a fixed time (after 100ns, for instance).

To analyze the die-to-die uniqueness in response, we model the process corners (fast, typical, and slow) by skewing the NW width and thickness by a factor of 10%, that is,

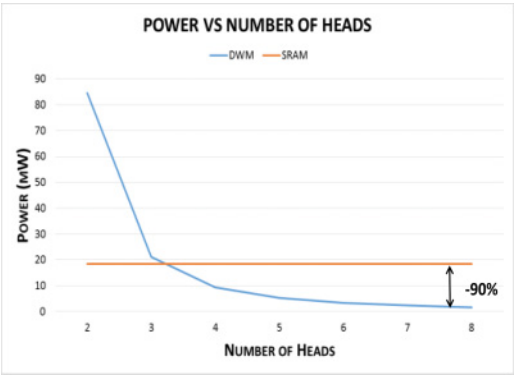


Fig. 11. Reduction in power, with respect to increase in number of heads, for a fixed number of challenges.

fast corner is (−10%, −10%) and slow corner is (+10%, +10%). Figure 10(b) shows the distribution of velocity for slow, typical, and fast corners. Again, the reference is selected to screen the pinned DWs for the three corners. We follow the similar simulation setup as described before for inter- and intra-HD analysis. The result is depicted in Figure 10(c). The average inter-HD is found to be 50%. For intra-HD, we note a long tail in the distribution is obtained due to sensitive bits (Figure 10(c)). An average of 45% separation between the interdie and the intra-HD is observed for memory-PUF.

4.3. Area and Power Estimation

Our simulations in 22nm PTM [ASU 2007] indicate that DW memory-PUF is 10X more power-efficient than SRAM-PUF when the number of sense points are increased to eight (Figure 11). Meaning, thereby, that each NW will provide eight responses, depending on read head selection. The footprint is better by an order of magnitude, considering a 2.56F2 footprint of DWM compared to a 140F2 for SRAM.

5. THREAT MODELS

In this section, we consider the resilience of the proposed PUFs against different threat models, such as machine learning or modeling-based attack and magnetic field attack [Jang et al. 2015]. We also present the limitations associated with the spintronic PUFs in this work.

5.1. Magnetic Attack

Figure 12(a) shows the MTJ schematic. MTJs are used as read and write heads in the DWM. By subjecting the MTJ to a strong external magnetic field, the information read can be corrupted. Figures 12(b) and (c) show that the MTJ-free layer could flip its polarity, either using current or with 250Oe magnetic field. The magnetic field produced by a common horseshoe magnet is approximately 126Oe, which is sufficient to flip the weak bits in the presence of process variations and thermal noise.

The attacks on MTJ could be launched through static (DC) magnetic field. The DC attack is less detrimental, as it can only create unipolar failures. For example, a magnetic field will cause failures only for the bits whose free-layer orientation is opposite to the applied field. The attack could be launched either during ideal (retention) mode or functional mode (read/write). Note that read current is unipolar, irrespective to the storage polarity, whereas write current polarity is data dependent. The impact of an attack during functional mode (especially read) could be more detrimental than retention due to two factors: (a) presence of disturb current, and (b) higher frequency of reads compared to writes. This can result in either a hard failure (i.e., flipping of bitcell

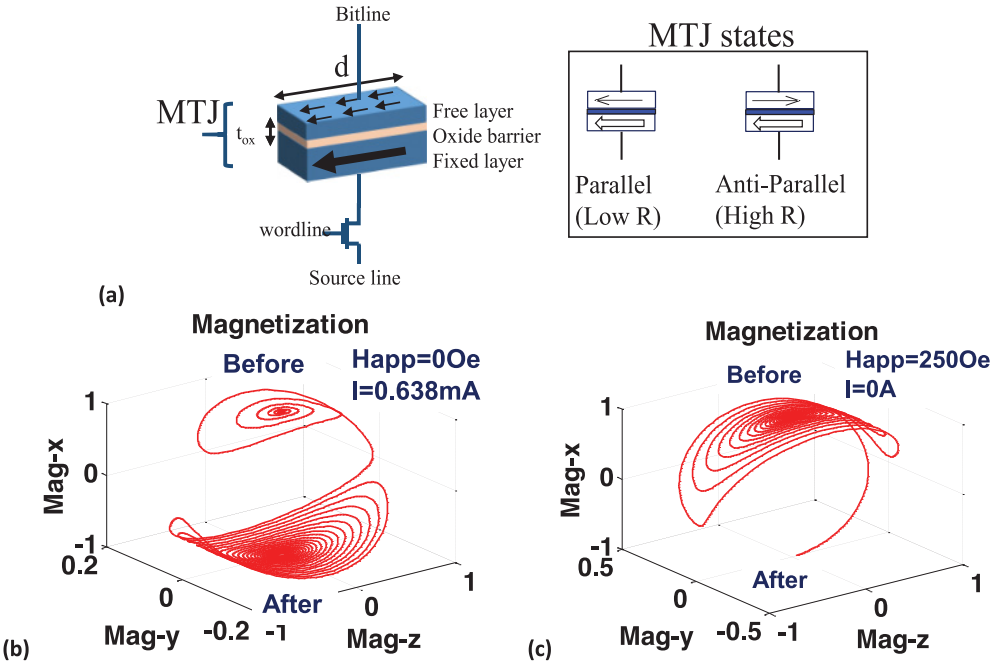
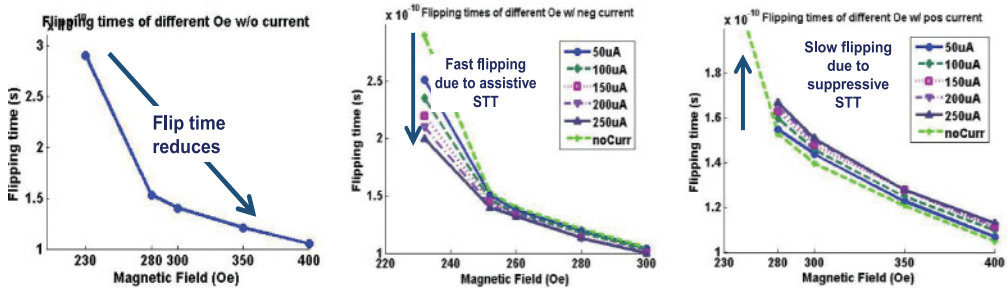


Fig. 12. (a) Schematic of MTJ, (b) flipping of MTJ due to STT (Happ = 0Oe, I = 0.638mA), and (c) due to external magnetic field (Happ = 260Oe, I = 0).



(a) (b) (c)

Fig. 13. Magnetic field impact on the stability of MTJ (free layer): under a (a) DC magnetic field. Impact of functional operation on the flip time in presence of (b) assistive current and (c) suppressing current.

content) or soft failure (i.e., delay in write or degraded sense margin). The soft failures could be mitigated by slowing down the read/write operation, but the hard failures need to be avoided or corrected through error correction. We use a publicly available micro-magnetic simulator, the Object Oriented MicroMagnetic Framework (OOMMF) [Donahue et al. 1999], to analyze the impact of DC magnetic field tampering on the integrity of the MTJ. For the simulation, we assume the MTJ parameters as shown in Table I. It can be noted from Figure 13(a) that the MTJ polarity could be flipped in retention mode. The flip time reduces with increasing strength of magnetic field. The comparison of MTJ stability between retention and functional mode is considered in Figures 13(b) and 13(c). For the analysis, we have assumed different magnitudes of read/write currents and polarities. It can be observed that the bits can fail easily

Table I. MTJ Parameters

Parameter	Value
Dimension	(60×120×3)nm
Damping constant (α)	0.01
Sat. Mag. (Ms)	1,000A/m
Exchange constant (A)	2e-11J/m
Polarization	0.8
Spin conductance	1e-3
Activation energy (Ea)	56kT
Anisotropy constant (Ku)	Ea/volume

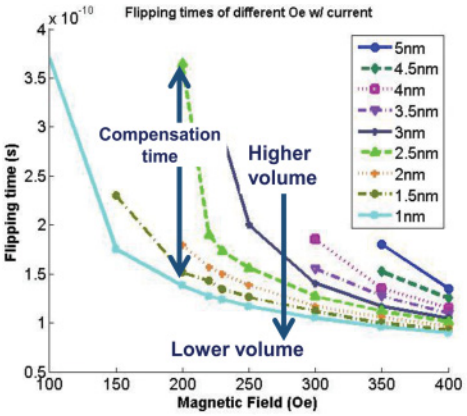


Fig. 14. Impact of MTJ volume on the flip time in presence of DC magnetic field.

when the current polarity and magnetic field are in the same direction (assistive). The flip time is higher when the current and magnetic field are in opposite directions (suppressive).

The stability of MTJ-free layer is a function of its volume. Therefore, it is possible to enhance the robustness of the MTJ against tampering by increasing the size. For this simulation, we have swept the MTJ thickness from 3nm to 0.5nm. Figure 14 plots the flip time with respect to the volume of free layer for DC attack. It can be observed that the bitcell is able to withstand weak magnetic attack with higher volume. However, it fails to provide protection against strong attack (>400Oe).

5.2. Machine Learning Attack

Machine learning deals with the ability of a computer algorithm to automatically learn a complex behavior from a limited set of observations (responses), and use this toward predicting the outcome (response) by generalizing the interactions of the device from these examples. PUFs are built upon a set of complex challenge-response pairs (CRPs) that exploit the underlying physical system with a limited number of unknowns. It must be noted that appropriate machine learning techniques must be employed to learn the behavior from a small training set of CRPs, and this is used toward making accurate predictions of unknown responses. In this work, we use 'Logistic Regression' implemented using the Waikato Environment for Knowledge Analysis (WEKA) [Oztiirk et al. 2008; Hall et al. 2009] for the analysis.

Logistic regression is a well-established machine learning framework, which is used to predict a binary response from a binary input. By measuring the relationship between the dependent variable and one or more independent variables, the probability of the output response is calculated and the appropriate output is predicted. In this work, we compare the traditional CMOS-based arbiter and SRAM PUF, with respect to DWM-based relay-PUF and memory-PUF. We use 75% of the CRPs toward training the machine learning algorithm and the remaining 25% toward the test. The probability of correct prediction for arbiter-PUF (relay-PUF) is 50.8% (48.4%), whereas for SRAM-PUF (memory-PUF), it is 65.6% (69.1%). Therefore, the proposed spintronic PUFs perform at par with the CMOS PUFs.

5.3. Other Possible Threat Models

Instances of invasive attack include disabling primitives partially or fully, tampering inputs to design, etc. Noninvasive attacks involve modulating the operating

environment (voltage, temperature) to trigger corner cases or kill the entropy momentarily, and side channel monitoring by exploiting operating modes (authentication vs normal).

5.4. Limitations of Spintronic PUFs

The PUF response is susceptible to environmental fluctuations and guaranteeing the repeatability of the PUF response could be challenging. The self-heating of NW may also alter the DW dynamics. These challenges will be studied in detail in the future and correction circuitries will be added to cancel these effects for improved robustness.

6. CONCLUSIONS

In this report, we proposed spintronic PUFs (modeling, circuit design, and analysis) for security, trust, and authentication. We reveal that nonlinear dynamics of the spintronic DW protects the proposed PUFs against machine learning based attacks. The NW dynamics allowed us to use different pulsing techniques that generate new challenge-response pairs, which enhance the strength of the proposed PUFs. The simulations show that DWM-PUFs can achieve 30% to 45% separation between intra- and inter-HD. New threat models, such as magnetic field–based attacks and environment modulation attacks, are also proposed.

REFERENCES

M. Abramovici and P. Bradley. 2009. Integrated circuit security: New threats and solutions. In *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies*. ACM, 55.

K. N. Alekseev, G. P. Berman, V. I. Tsifrinovich, and A. M. Frishman. 1992. Dynamical chaos in magnetic systems. *Soviet Physics Uspekhi* 35, 7, 572.

A. J. Annunziata, M. C. Gaidis, L. Thomas, C. W. Chien, C. C. Hung, P. Chevalier, et al. 2011. Racetrack memory cell array with integrated magnetic tunnel junction readout. In *2011 International Electron Devices Meeting*.

ASU. 2007. Predictive Technology Model. Retrieved from http://ptm.asu.edu/.

Supriyo Bandyopadhyay and Marc Cahay. 2008. *Introduction to Spintronics*. CRC Press, Boca Raton, FL.

B. Behin-Aein, D. Datta, S. Salahuddin, and S. Datta. 2010. Proposal for an all-spin logic device with built-in memory. *Nature Nanotechnology* 5, 4, 266–270.

L. Berger. 1984. Exchange interaction between ferromagnetic domain wall and electric current in very thin metallic films. *Journal of Applied Physics* 55, 6, 1954–1956.

M. J. Donahue and D. G. Porter. 1999. *OOMMF User's Guide*. US Department of Commerce, Technology Administration, National Institute of Standards and Technology.

A. Driskill-Smith. 2010. Latest advances and future prospects of STT-RAM. In *Proceedings of the Non-volatile Memories Workshop*.

R. A. Duine, A. S. Núñez, and A. H. MacDonald. 2007. Thermally assisted current-driven domain-wall motion. *Physical Review Letters* 98, 5, 056605.

P. P. Freitas and L. Berger. 1985. Observation of s-d exchange force between domain walls and electric current in very thin permalloy films. *Journal of Applied Physics* 57, 4, 1266–1269.

M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. H. Witten. 2009. The WEKA data mining software: an update. *ACM SIGKDD Explorations Newsletter* 11, 1, 10–18.

Masamitsu Hayashi. 2006. *Current Driven Dynamics of Magnetic Domain Walls in Permalloy Nanowires*. PhD dissertation, Stanford University.

D. G. Hermann and J. P. Nguenang. 2013. Chaos Appearance during Domain Wall Motion under Electronic Transfer in Nanomagnets.

D. E. Holcomb, W. P. Burleson, and K. Fu. 2009. Power-up SRAM state as an identifying fingerprint and source of true random numbers. *IEEE Transactions on Computers* 58, 9, 1198–1210.

A. Iyengar, K. Ramclam, and S. Ghosh. 2014. DWM-PUF: A low-overhead, memory-based security primitive. In *Proceedings of the 2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. IEEE, 154–159.

A. Iyengar, S. Ghosh, and K. Ramclam. 2015. Domain wall magnets for embedded memory and hardware security. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems* 5, 1 (2015), 40–50.

J. Jang, J. Park, S. Ghosh, and S. Bhunia. 2015. Self-correcting STTRAM under magnetic field attacks. In *52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*. IEEE, 1–6.

M. Jamali, K. J. Lee, and H. Yang. 2012. Metastable magnetic domain wall dynamics. *New Journal of Physics* 14, 3, 033010.

B. Jun and P. Kocher. 1999. *The Intel Random Number Generator.* Cryptography Research Inc. White Paper.

A. Maiti, J. Casarona, L. McHale, and P. Schaumont. 2010. A large scale characterization of RO-PUF. In *Proceedings of the 2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. IEEE, 94–99.

R. Nebashi, N. Sakimura, Y. Tsuji, S. Fukami, H. Honjo, S. Saito, et al. 2011. A content addressable memory using magnetic domain wall motion cells. In *Proceedings of the 2011 Symposium on VLSI Circuits (VLSIC)*. IEEE, 300–301.

D. Nikonov and G. Bourianoff. 2006. Taxonomy of spintronics (a zoo of devices). Retrieved from http://nanohub.org/resources/1940.

H. Okuno. 1997. Chaos and energy loss of nonlinear domain wall motion. *Journal of Applied Physics* 81, 8, 5233–5235.

E. Ott. 2002. *Chaos in Dynamical Systems*. Cambridge University Press.

E. Oztiirk, G. Hammouri, and B. Sunar. 2008. (March). Towards robust low cost authentication for pervasive devices. In *Proceedings of the 6th Annual IEEE International Conference on Pervasive Computing and Communications (PerCom'08)*. IEEE, 170–178.

R. Pappu. 2001. *Physical One-Way Functions*. PhD thesis, Massachusetts Institute of Technology.

S. S. Parkin, M. Hayashi, and L. Thomas. 2008. Magnetic domain-wall racetrack memory. *Science* 320, 5873, 190–194.

J. Rajendran, R. Karri, J. B. Wendt, M. Potkonjak, N. R. McDonald, G. S. Rose, and B. T. Wysocki. 2012. Nanoelectronic solutions for hardware security. *IACR Cryptology Eprint Archive* 2012, 575.

G. S. Rose, D. Kudithipudi, G. Khedkar, N. McDonald, B. Wysocki, and L. K. Yan. 2014. Nanoelectronics and hardware security. In *Network Science and Cybersecurity*. Springer, New York, 105–123.

M. Rostami, F. Koushanfar, J. Rajendran, and R. Karri. 2013. (November). Hardware security: Threat models and metrics. In *Proceedings of the International Conference on Computer-Aided Design.* IEEE Press, 819–823.

Samsung. 2013. SGMI Research Themes & Subjects. Online: http://www.samsung.com/global/business/semiconductor/html/news-events/file/SGMI_Proposal_Guide_and_Format_R1.pdf.

S. Srinivasan. 2012. *All Spin Logic: Modeling Multi-Magnet Networks Interacting Via Spin Currents*. PhD dissertation, Purdue University.

T. Tanamoto, N. Shimomura, S. Ikegawa, M. Matsumoto, S. Fujita, and H. Yoda. 2011. High-speed magnetoresistive random-access memory random number generator using error-correcting code. *Japanese Journal of Applied Physics* 50, 4S, 04DM01.

A. Thiaville and Y. Nakatani. 2006. Domain-wall dynamics in nanowiresand nanostrips. In *Spin Dynamics in Confined Magnetic Structures III*. Springer, Berlin, 161–205.

P. Tuyls, G. J. Schrijen, B. Škorić, J. Van Geloven, N. Verhaegh, and R. Wolters. 2006. Read-proof hardware from protective coatings. In *Cryptographic Hardware and Embedded Systems (CHES'06)*. Springer, Berlin, 369–383.

S. X. Wang and A. M. Taratorin. 1999. *Magnetic Information Storage Technology: A Volume in the Electromagnetism Series*. Academic Press.

Y. Wang, W. K. Yu, S. Wu, G. Malysa, G. E. Suh, and E. C. Kan. 2012. Flash memory for ubiquitous hardware security functions: True random number generation and device fingerprints. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy (SP).* IEEE, 33–47.

S. A. Wolf, D. D. Awschalom, R. A. Buhrman, J. M. Daughton, S. Von Molnar, M. L. Roukes, et al. 2001. Spintronics: A spin-based electronics vision for the future. *Science* 294, 5546, 1488–1495.

S. H. Yang, K. S. Ryu, and S. Parkin. 2015. Domain-wall velocities of up to 750 m s^{-1} driven by exchange-coupling torque in synthetic antiferromagnets. *Nature Nanotechnology* 10, 3 (2015), 221–226.

J. Zhang, P. M. Levy, S. Zhang, and V. Antropov. 2004. Identification of transverse spin currents in noncollinear magnetic structures. *Physical Review Letters* 93, 25, 256602.

Y. Zheng, A. R. Krishna, and S. Bhunia. 2013. (January). ScanPUF: Robust ultralow-overhead PUF using scan chain. In *Proceedings of the 2013 18th Asia and South Pacific Design Automation Conference (ASP-DAC).* IEEE, 626–631.

I. Žutić, J. Fabian, and S. D. Sarma. 2004. Spintronics: Fundamentals and applications. *Reviews of Modern Physics*, 76, 2, 323.

Received December 2014; revised May 2015; accepted July 2015