CONTRIBUTED PAPER

Spintronics and Security: Prospects, Vulnerabilities, Attack Models, and Preventions

Spintronic devices gather a number of entropy sources which can be advantageously used for hardware security. The spatial and temporal randomness in the magnetic systems can complement the existing CMOS-based security and trust infrastructures to realize novel hardware security primitives such as physical unclonable functions, encryption engines, and true random number generators.

By Swaroop Ghosh, *Senior Member IEEE*

ABSTRACT | The experimental demonstration of current-driven spin-transfer torque (STT) for switching magnets and push domain walls (DWs) in magnetic nanowires have opened up new avenues for spintronic computations. These devices have shown great promise for logic and memory applications due to superior energy efficiency and nonvolatility. It has been noted that the nonlinear dynamics of DWs in the physical magnetic system is an untapped source of entropy that can be leveraged for hardware security. The inherent noise, spatial, and temporal randomness in the magnetic system can be employed in conjunction with microscopic and macroscopic properties to realize novel hardware security primitives. Due to simplicity of integration, the spintronic circuits can be an add-on to the silicon substrate to complement the existing CMOS-based security and trust infrastructures. This paper investigates the prospects of spintronics in hardware security by exploring the security-specific properties and novel security primitives realized using spintronic building blocks. As spintronic elements enter the mainstream computing platforms, they are exposed to emerging attacks that were infeasible before. This paper covers the security vulnerabilities, security and privacy attack models, and possible countermeasures to enable safe computing environment using spintronics.

KEYWORDS | Chaos; data privacy; data security; domain-wall memory (DWM); encryption engines; hardware security; magnetic RAM (MRAM); nanowire; physically unclonable functions; spin-transfer-torque RAM (STTRAM); spintronics; true random number generator

I. INTRODUCTION

Satisfying the functionality, frequency, and thermal design power (TDP) requirements in today's highly integrated circuits and systems is not adequate. Ensuring the trustworthiness and security of the design parts and overall system is the *de facto* component of the design goal. This is largely due to the profit-driven business model that involves "untrusted" third party in every step of integrated circuit (IC) manufacturing process—from design, synthesis, and layout all the way to fabrication and packaging. The latest trend of integrating third-party intellectual property (IP) blocks in the system makes the problem more intricate. Broadly, the attacks [1]–[7] could fall under: 1) malicious modifications: malwares such as hardware Trojans can be inserted in the ICs which leak information, cause denial-of-service, or malfunction once triggered to name a few; 2) cloning/fake IC: the adversary can copy the design, fabricate and sell at discounted price to lower the profit margin of the genuine design; 3) hacking/snooping: the adversary snoops the communication in the channel to crack the secret key for malicious intent such as impersonation, hacking etc.; 4) side channel attacks: side channels, e.g., current and voltage, are monitored to leak the secret information

Manuscript received August 26, 2015; revised March 8, 2016; accepted May 23, 2016. Date of publication September 2, 2016; date of current version September 16, 2016. This work was supported in part by the National Science Foundation under Grant CNS-1441757 and the Semiconductor Research Corporation under Grant 2442.001.
The author is with the School of Electrical Engineering and Computer Science, Pennsylvania State University, University Park, PA 16801 USA (e-mail: szg212@psu.edu).

Digital Object Identifier: 10.1109/JPROC.2016.2583419

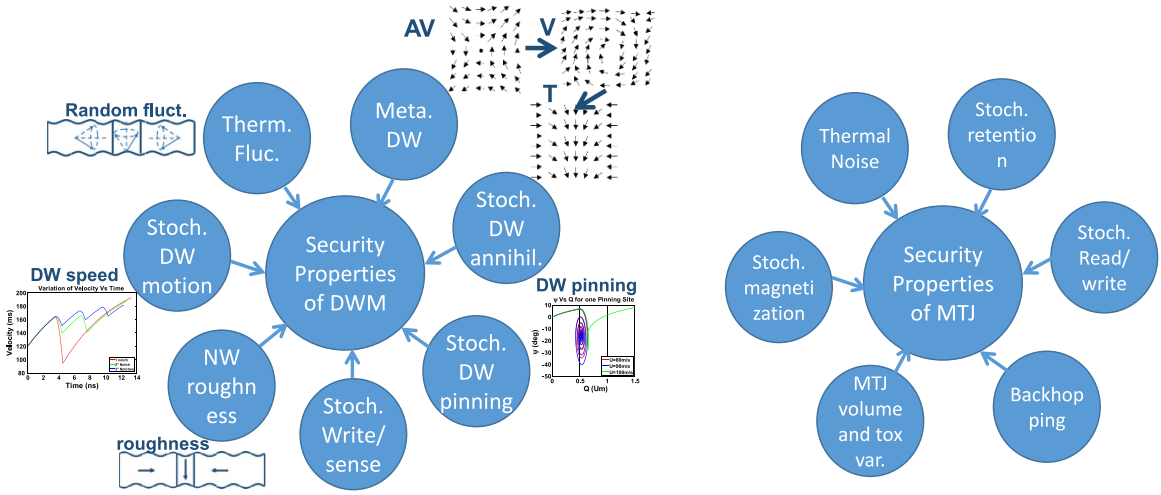

Fig. 1. ***Sources of entropy and randomness in spintronic systems such as DWM and MTJ.***

and extract secret keys; 5) reverse engineering: the design details are decoded, IC is hacked, and secret information is stolen; and 6) IC recycling: the discarded ICs from unused boards are recycled at lower price for profitability. In this context, it is worth mentioning that 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 ICs. The need for authentication is further amplified due to eavesdropping on the communication channel. The worldwide security technology and services market is expected to cross $67 billion by 2013 [8], underscoring the importance of security.

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 while uncovering and solving emerging security issues such as Trojan insertion, IC recycling, chip cloning, and side channel attacks. 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 CMOS-based circuits are area and power overhead, sensitivity to environmental fluctuations and limited randomness and entropy offered by the Silicon substrate. Emerging technologies such as spintronics have shown promises to bring abundance of entropy and physical randomness while being robust, fast and orders of magnitude energy-efficient than CMOS [153]–[155], [160].

The experimental results on spin valves, magnetic-tunnel junctions (MTJs), domain-wall memory (DWM), etc. [84]–[134] 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. The thermally activated electrons in the material add to the entropy. Besides, the magnet is also sensitive to physical randomness. Fig. 1 captures the sources of entropy and randomness possessed by spintronic systems such as DWM and MTJ (discussed in Section II-A). It has been noted that the magnetization dynamics is typically nonlinear in nature. For example, DW motion in the rough nanowire making it resistant to modeling-based attacks that are prevalent in CMOS-based security primitives [155]. The unique features such as shift-based access and energy-efficient computation leads to easy adoption of spintronic devices for primitives such as encryption engines, TRNG, PUF, and so on.

Although spintronic technology is excellent choice for the design of hardware security primitives, the regular spintronic circuits and memory may be easy targets for carefully orchestrated attack. Such attacks exploit the fact that majority of spintronic devices are fundamentally susceptible to ambient parameters such as magnetic field, temperature, and laser heating. Furthermore, the spintronic devices are nonvolatile making the data persistent. Therefore, the circuits, specifically memory, designed using spintronics bring new security challenges that were absent in their conventional volatile memory counterparts such as static RAM (SRAM) and embedded dynamic RAM (eDRAM) [158]. The root cause is persistent data that may allow the adversary to retrieve sensitive information like password or cryptographic keys and the fundamental dependency of the memory technology on ambient parameters such as magnetic field and temperature that can be exploited for low-cost tampering. There are two aspects to NVM security.

1) Data integrity: It pertains to data corruption (functional or timing) or destruction by malicious attack

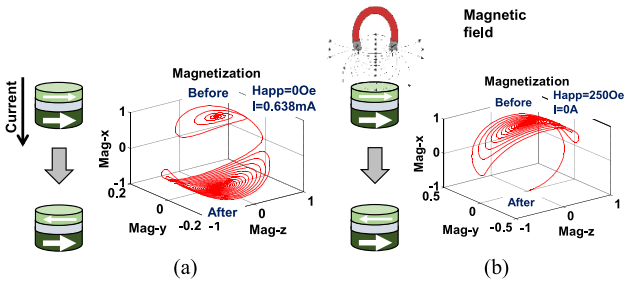

Fig. 2. *(a) Flipping of MTJ free layer due to STT (***Happ** = **0Oe**, ***I*** = **0.638mA***). (b) Due to external magnetic field (***Happ*** = **250Oe**, ***I*** = **0***). The plots are obtained by solving LLG from (1).*

with the intention to launch denial-of-service. The magnets such as free layer of MTJ and domain walls in DWM could be toggled through both spin polarized current as well as magnetic field. Therefore it is susceptible to manipulation through both the magnitude and polarity of external magnetic field. Fig. 2(a) and (b) show that the MTJ free layer could flip its polarity either using current or with 260Oe magnetic field. The magnetic field produced by a common horseshoe magnet is ~250Oe [161] which is sufficient to flip the weak bits in presence of process variations and thermal noise. The same effect could also be obtained through temperature modulation and localized laser heating. Protecting data integrity against malicious attacks through ambient effect is particularly critical on deployed systems that are hard to maintain and enforce physical security.

2) Data privacy: It pertains to sensitive data being compromised. One possible scenario is when the tag bits are persistent throughout the power cycle and a malicious read operation by attacker at power-ON results in cache hit in NVM last level cache (LLC), giving away sensitive information such as keys, passwords, and account numbers. The desire to have larger LLC for performance gain presents more persistent data that is vulnerable to attack. Storage such as hard disk drive (HDD) has been the nonvolatile part of memory system. Many efficient solutions (mostly based on encryption) [162] exist that address its security and privacy. As nonvolatility is introduced at higher levels of memory stacks (that traditionally were volatile) more data become vulnerable that were safe before. The primary challenge associated with addressing data privacy in higher levels of memory stack is performance. Closer the memory level is to CPU, the more sensitive it is to latency. Consequently, the latency associated with encryption and authentication that is used for storage is not trivial in LLC. Another issue is energy overhead of the protection. Designing a magnetic or heat shield around the device is the first solution. Considering the cost and weight of magnetic shield, it may not be practical.

The data privacy aspect of NVM security is addressed to some extent by semi nonvolatile memory (SNVM) which is similar to NVM memory but with very low retention time [151]. The retention time is intentionally lowered to improve latency and power. Additionally, it provides better privacy as the data vanishes after power is turned OFF. Nevertheless, attacks of following types could be still be launched on the LLC: 1) malicious access at power-ON to read the persistent information; 2) contactless tampering through external electromagnetic field, temperature, and laser; and 3) probing and scanning between power cycles. This paper reviews some of the latest literature on vulnerabilities, attack models and preventive solutions associated with spintronic memory.

The remainder of this paper is organized as follows. Section II provides background on hardware security primitives and desired features required from the underlying technology. Different flavors of spintronic devices and the security features offered by them are also covered. Section III focuses on the security primitives designed using spintronics. The data security issues associated with spintronics and possible countermeasures are described in Section IV. Data privacy issues and possible countermeasures are presented in Section V. The future directions are presented in Section VI. Finally, conclusions are drawn in Section VII.

II. BACKGROUND

Here, we describe various flavors of hardware security primitives and the desirable features from the underlying technology. Next, we review some of the well-known spintronic devices, their operating principles, and the security-specific properties.

A. Hardware Security Primitives

1) Recycling Sensor: Chip recycling involves scavenging and reusing the aged but functionally correct ICs in new systems. Although the machines might operate correctly, the operating speed and energy efficiency will be degraded due to prior usage. Detecting recycled ICs are essential to improve the security and trustworthiness of the integrated systems. The conventional techniques exploit the temporal degradation of circuit performance to isolate the recycled ICs [47]–[49]. These techniques rely on aging mechanisms such as bias temperature instability (BTI) and hot-carrier injection to degrade the ring oscillator (RO)-based sensor circuit. The performance degradation of degraded RO is compared with the fresh RO to identify the recycled ICs. One of the primary challenges in recycling detection is the process variation between

the aged (or stressed) and fresh RO at $t = 0$. There are two possibilities: Case-1: stressed RO is slower than fresh RO where the chip will be falsely identified as "recycled"; and Case-2: stressed RO is faster than fresh RO where fine grained recycling of the chip will be masked. Isolating the recycled ICs from the genuine ones for arbitrarily small amount of usage (few seconds to minutes) is a challenging task.

Key requirements are low process variation, high sensitivity to temporal degradation, or unique signature of usage.

2) True Random Number Generator (TRNG): True random number generator (TRNG) [65]–[83] is the crucial component of encryption engines. It is typically employed instead of software based random numbers for key generation. Due to limited throughput of hardware TRNG they are also used to generate seeds for a faster cryptographically secure pseudorandom number generator. There is a direct relationship between the strength of encryption and the seed random number. TRNG harnesses the natural entropy present in the system such as thermal noise [65]–[68], shot noise, Brownian motion or nuclear decay [69]. Techniques to harvest/capture the noise in the operational amplifier [70], [71], jitter of coupled oscillators [72]–[75], state of bi-stable elements [76]–[78] and oxide breakdown of transistors [79], [80] have also been proposed. The challenges involved in designing TRNG involve exploiting new entropy sources (e.g., introducing SiN in the channel or nanodevices [81], [82]), using efficient harvesting mechanisms to extract the entropy and careful postprocessing to eliminate the errors introduced in the entropy source and collection process. Other factors are repeatability, unpredictability, throughput, power consumption, robustness, and resilience to attacks.

Key requirements are high entropy, nonlinearity, high bandwidth (bits/s), and energy efficiency (joules/bit).

3) Physically Unclonable Function (PUF): PUF [26]–[29] is one of the security primitives to prevent cloning of chips. Note that techniques, such as logic encryption and camouflaging/logic obfuscation [148], also exist to resist against reverse engineering and potential cloning. PUF replaces the hard-coded key in the IC with specifically designed circuits that work on the principle of challenge-response. The response to a particular challenge is based on the physical properties of the chip (e.g., process). The unclonability of the PUF makes the response hard to predict by the adversaries. Several flavors of PUFs, e.g., optical PUF [30], delay PUF [31]–[34], SRAM PUF [35]–[38], flash PUF [39], and flip-flop PUF [40], have been proposed in literature. Arbiter-PUF [32] is one of the earliest form of PUF design. It contains an arbiter and two identically designed delay paths. Note that, in contrast to the arbiter that is conventionally used in computer architecture for scheduling, the arbiter used in PUF picks the fast arriving signal to set the response. During authentication, a signal is raced in two parallel paths (the exact path is determined by the challenge). The response is generated by comparing the delays of the two paths in race. The delay difference is converted to 0 or 1 response. Arbiter-PUF banks on the fact that the path delays will differ due to process variations. Therefore, the PUF response is random in nature. This scheme also employs delay difference to minimize environmental fluctuation (i.e., temperature and voltage variation) induced errors. Some of the key PUF design requirements are as follows.

1) High inter-die variability in response: The PUF response for the same challenge should show high variability between two different dies. This will ensure that the chip can be uniquely identified.
2) Low intra-die variability in response: The PUF response for the same challenge should be stable under environmental fluctuations and consecutive accesses. This requirement is related to repeatability which requires that the PUF response should be stable for a given challenge after the enrollment phase (i.e., the PUF responses to all challenges when used for the first time). Hamming Distance (HD) [163] is a widely used metric to characterize the PUF's quality including but not limited to inter and intra-die variability.
3) Balanced 0/1 response: The PUF response should be balanced between '0' and "1" for all challenges. This will ensure that the PUF response cannot be predicted easily. Although this is one of the popular metric in the PUF literature, it is not an absolute requirement.
4) Throughput, energy and area: The throughput of PUF is measured in terms of number of response bits produced per second whereas energy is measured as energy consumed per bit response. The area and power of the PUF should be low while the throughput is expected to be high.

In order to meet requirements 1) and 2) mentioned above, the PUF should be sensitive to process variations. The responses of the PUF that are closer to the boundary between 0 and 1 might move under environmental fluctuations causing errors. However, if the process variations is large the PUF responses will stay away from the boundary making them immune to minor voltage and temperature fluctuation.

Key requirements are large process variation, nonlinearity, insensitivity to temporal degradation, high bandwidth (bits per second), energy efficiency (joules per bit).

4) Encryption Engines: Encryption is a widely used methodology to protect the data against snooping and impersonation. Among the encryption standards, the Advanced Encryption Standard (AES) [50] is the widely accepted algorithm. For better throughput, AES is typically implemented in hardware, e.g., FPGA [51]–[54] and ASIC [55]–[58]. Due to complexity of AES implementation,

Table 1 Hardware Security Primitives, Key Requirements and Properties Offered by Spintronics

Security primitive	Key Requirements	Features offered by spintronics
Recycling sensor	Low process variation, high sensitivity to usage	DW nucleation
PUF	High process variation, nonlinearity	Stochastic DW motion in rough nanowire, nonlinearity
TRNG	High entropy	Noise sensitivity of magnetization, stochastic dynamics
Encryption	Recursive shift, multiplication, addition	Shift-based computation
Miscellaneous	Sensitivity to ambient parameters	Sensitivity to magnetic field, temperature

specialized architecture of individual components such as S-box and column-mixing [59]–[62] has also been proposed. Since hardware encryption is side channel attack target, several attack-resistant designs have also been introduced [63], [64]. The AES encryption process contains four basic operations on 128 b of plaintext that is organized as 4×4 array (each consisting 1 byte data) called state matrix (SM). Depending on the key length a specified number of rounds are performed on the plaintext. The AES rounds consist of the following transformations.

1) SubByte: This is a nonlinear substitution operation where each byte of SM is replaced using the same substitution function (S-box). This step is compute (leakage) intensive for logic (memory based look-up table) implementation.
2) ShiftRows: This operation rotates each row cyclically to the left by the amount equal to the row number. The goal of this transformation is to scramble the byte order inside the 128-bit block.
3) MixColumns: This transformation maps each column of the SM to a new column by multiplying it by a matrix containing numbers 1, 2, and 3 (9, 11, 13, 14 for decryption). These operations could be achieved by shift and add e.g., 13X is $(8X + 4X + 1X)$ and addition can be implemented using XOR and NAND/NOR gates. The goal is to further scramble the 128-b block.
4) AddRoundKey: This step XORs the SM with the round key.

From the above, it is evident that AES requires extensive shift and XOR operations. Therefore, technologies offering low-overhead shift and XOR operation may benefit the AES engines.

Key requirements are serial access, high-quality TRNG, energy-efficient XOR, and addition.

5) Miscellaneous Primitives: Besides the security primitives described above several other primitives can be used to ensure the security and privacy of broad range of electronic parts. These may include Identification (ID), tamper sensor, pressure sensor, thermal sensor, ultra-wideband [164] and so on. The corresponding features required may be temperature, pressure and tamper sensitivity.

B. Spintronic Elements and Security Properties

Table 1 summarizes the key requirements of security primitives and features offered by spintronics. The details are provided as follows.

1) Magnetic Tunnel Junctions:

A. Technology: Magnetic tunnel junction (MTJ) contains a free layer and a pinned magnetic layer [a schematic is shown in Fig. 3(a)]. The resistance of the MTJ stack is high (low) if the free layer magnetic orientation is antiparallel (parallel) compared to the fixed layer. The configuration of the MTJ can be changed from parallel (P) to antiparallel (AP) or *vice versa*. The switching of free layer is achieved by field-driven or current-driven techniques. The field-driven MTJ is the basis for MRAM technology [168] which is promising due to high-density, low standby power, and high-speed operation. STTRAM [167] is energy-efficient variant of MRAM where the switching of magnetization is based on spin-transfer-torque using current. Fig. 3(a) and (b) shows the schematic of MRAM and STTRAM bitcell, respectively. In MRAM, a torque in appropriate polarity is induced on the free layer of the MTJ during write by generating fields through digitline and bitline (the isolation transistor is kept off). In STTRAM, the write done by injecting current from the source-line to the bitline or vice versa. The dynamics of free-layer magnetization is governed by Landau Liftshiftz Gilbert (LLG) equation [120], [121] as follows:

$$\frac{\partial \vec{m}}{\partial t} = -\gamma \vec{m} \times \left(H_{\text{eff}} + \underbrace{h_{\text{st}}}_{\text{stochastic}} \right) - \alpha\gamma \vec{m} \times \left[\vec{m} \times \left(H_{\text{eff}} + \underbrace{h_{\text{st}}}_{\text{stochastic}} \right) \right] + \underbrace{\frac{I_s \hbar G(\psi)}{2e} \vec{m} \times (\vec{m} \times \vec{e_p})}_{\text{STT}} \quad (1)$$

where $\vec{m}$ is unit vectors representing local magnetic moment, α represents the Gilbert's damping parameter, γ is gyromagnetic ratio, h_{st} is field due to stochastic noise, I_s is

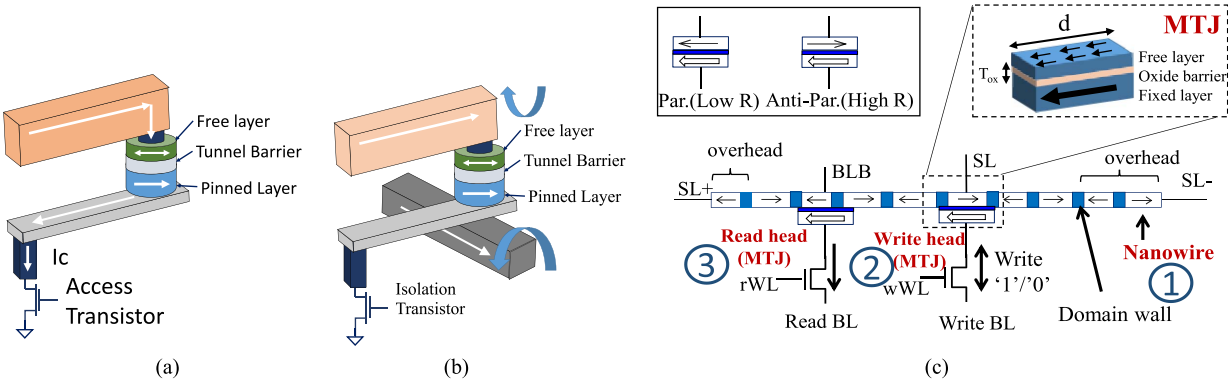

Fig. 3. *Schematic of (a) STTRAM; (b) MRAM; and (c) DWM bitcells.*

spin current, $G(\psi)$ is the transmission coefficient, $\hbar$ is reduced planck's constant, e is charge on electron, and $\overrightarrow{e_p}$ is the unit vector along fixed layer magnetization. In the above expression H_{eff} is an effective field given by $\overrightarrow{H_{\text{eff}}} = \overrightarrow{H_a} + \overrightarrow{H_k} + \overrightarrow{H_d} + \overrightarrow{H_{\text{ex}}}$, where H_a is the applied field, H_k is the anisotropy field, H_d is the demagnetization field, and H_{ex} is exchange field.

The retention time of the MTJ, i.e., the time between which the free layer magnetization tends to flip, is given by $T_{\text{ret}} = f_0 * e^{\Delta}$ where f_o is the thermal attempt frequency, which is roughly 1 GHz. Thermal energy $\Delta = (K_u V/k_B T)$ where K_u is the magneto-crystalline anisotropy, V is the volume of the free layer, T is the operating temperature, and k_B is the Boltzmann constant. By injecting a small amount of current (I) into the MTJ, the retention time can be altered as follows [191]:

$$\Delta = \left(\frac{K_u V}{k_B T}\right)\left(1 - \frac{I}{I_{\text{co}}}\right). \tag{2}$$

Note that (1) and (2) are crucial to understanding the factors that can influence the magnetization dynamics and retention time of MTJ. These factors can be employed by designers to design high-quality security primitives (see Sections III-A and III-C), whereas the same can be exploited by the hackers to tamper with the circuit functionality (Sections V-A and V-C).

B. Security Properties: Fig. 1(b) summarizes the security-specific properties of MTJ.

1) Chaotic magnetization: The dynamics of MTJ free layer is chaotic especially at the bifurcation point (i.e., at the border of P and AP states) [15]. It can be noted that chaos is deterministic for a given initial point. However, the behavior of chaotic system is very sensitive to the initial point which makes it unpredictable especially when the initial point contains variation [190]. This feature makes chaos a suitable property for hardware security.
2) Statistical read and write failures [184]–[186]: The MTJ critical current is a function of thermal energy (Δ) which in turn is a function of free layer volume. Higher Δ increases the critical write current (which increases the write latency and write failures) but improves the robustness of MTJ to read disturb failure. Vice versa is true for the lower Δ. Therefore, process variations can result in statistical variation in read and write failure rates which can be exploited for PUF design.
3) Statistical and stochastic retention: The MTJ retention time is a function of Δ (higher Δ increases the retention time). Therefore, the retention time is statistical under process variation [184]. The retention time is also stochastic in nature. The mean retention time is given by Δ whereas the actual value is a function of noise and environmental conditions. The precession of free layer is also stochastic (a function of damping, effective field, current and thermal noise) which results in MTJ resistance variation both in P and AP states.
4) Back-hopping: It has been experimentally shown that the free layer magnetization can flip back and forth (known as back-hopping phenomena) under high bias across the MTJ [9]. Back-hopping is one of the crucial challenges for applicability of large scale STTRAM arrays [10]. The back-hopping switching probability function for AP to P switching with initial condition of $P_1(t=0) = 0$ is given by [9]

$$P_1 = \frac{\gamma_1}{\gamma_1 + \gamma_2}\left\{1 - \exp[-(\gamma_1 + \gamma_2)t]\right\}$$

and

$$\gamma_{1,2} = \gamma_0 \exp\left[\frac{C}{k_B T}(H_k \mp H)^2\left(1 \mp \frac{V}{V_c}\right)\right] \tag{3}$$

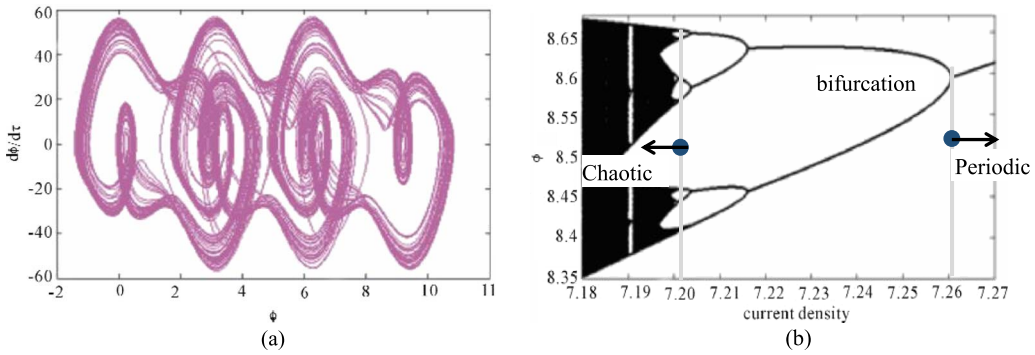

Fig. 4. *Chaos in magnetic systems [126] (a) DW speed with phase. (b) Bifurcation of DW with current density (reproduced with permission).*

where $CH_k^2(H_k \mp H)^2 = E_0$ is the free layer shape anisotropy, V_c is the spin-torque switching threshold at zero temperature, and $\gamma_0 = 10^9$ Hz is the attempt frequency.

Due to highly entropic response back-hopping can be potentially useful for random number generation.

2) Magnetic Nanowire in DWM:

A. Technology: DWM is a promising memory technology due to its multi-level cell capability, allowing it to store multiple bits per cell [100]–[104], [165], [166] [Fig. 3(c)]. Additionally, it provides low standby power, non-volatility, fast access time, good endurance, and good retention. DWM consists of three components: 1) the read head; 2) the write head; and 3) a magnetic nanowire. The read and write heads are similar to conventional MTJs, while the nanowire holds the bits in terms of magnetic polarity. 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 prospect of current induced motion of DWs [111]–[118] in the ferromagnetic films has created significant interest for high-density memory application where bits are stored analogous to hard disk [119]. The DWs can be shifted forward and backward by injecting charge current from left-shift and right-shift contacts, causing the nanowire to operate as a shift register. The new domains are injected by first pushing current through shift contacts to move the bits in lockstep until the desired bit is under write head. Next, spin-polarized current is injected through the write MTJ (using wWL, wBL and SL) in a positive or negative direction to write a "1" or "0" (up-spin or down-spin) in the nanowire. A read is performed by bringing the desired bit under read head using a shift and sensing the resistance of the MTJ formed by the new bit (after the DW crosses the read head) using rBL and rWL. 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 LLG equation [120], [121]. The modified LLG of the DW with stochastic magnetic field is given by

$$\frac{\partial \vec{m}}{\partial t} = -\gamma \vec{m} \times \left(H_{\text{eff}} + \underbrace{h_{\text{st}}}_{\text{stochastic}} \right) + \alpha \vec{m} \times \frac{\partial \vec{m}}{\partial t} - u(\vec{j} \cdot \nabla)\vec{m} + \beta u \vec{m} \times (\vec{j} \cdot \nabla)\vec{m} \quad (4)$$

where $\vec{m}$ and $\vec{j}$ are unit vectors representing local magnetic moments and current flow. α, β, and γ represent the Gilbert's damping parameter, the non-adiabatic spin transfer term, and gyromagnetic ratio respectively. The effective field is represented by $H_{\text{eff}} = -(1/\mu_0 M_s)(\delta w/\delta \vec{m})$ and the field due to stochastic noise is h_{st}. The parameter u is the spin transfer torque parameter, and it is proportional to the current density J, the spin polarization P, and is given by $u = \mu_B JP/eM_s$, where M_s is the saturation magnetization, w is the energy density, and μ_B is the Bohr magnetron.

Although the discussion in this paper is limited to DWM, STTRAM, and MRAM it should be noted that several other flavors of spintronic memory technologies have also been proposed in literature. Some examples include DWM with single DW, spintronic memristor, magnetic Quantum Cellular Automata (QCA), spin gain transistor, a spin Hall effect (SHE) device, and so on [92]. In theory, these devices could also be explored from a security standpoint.

B. Security Properties: Besides entropy, the DWM possesses several microscopic and macroscopic properties [155] as described below [Fig. 1(a)].

Microscopic Properties:

1) Chaotic dynamics: The likelihood of chaos appearance during domain wall motion under electrical current has been studied in [126]–[132]. Bifurcation analysis and existence of positive Lyapunov parameter for certain values of damping constant

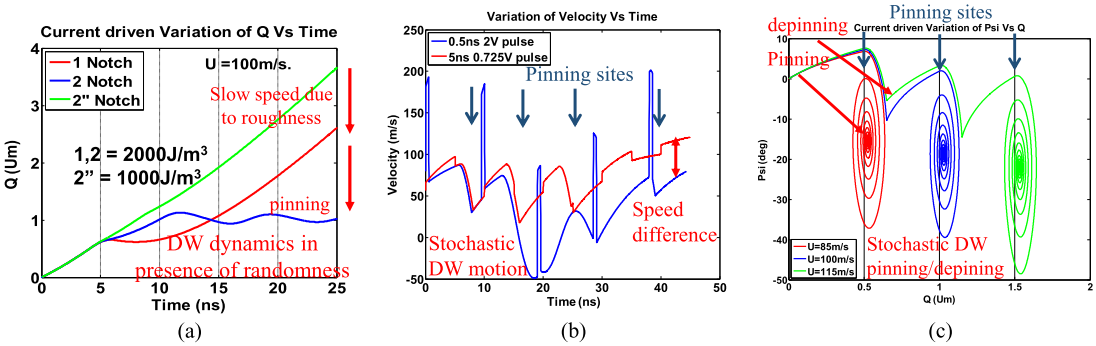

Fig. 5. *(a) DW dynamics in presence of physical roughness induced slowdown and eventual pinning. (b) Stochastic motion of DW. A misaligned shift pulse reduces velocity. (c) DW dynamics with two different shift current magnitude and duty cycle but same average value is also shown. Stochastic pinning of DWs with respect to three different shift currents [153].*

indicate the presence of chaos in DW motion. Fig. 4(a) shows the dynamics in the phase space when damping parameter lies in chaotic regime. The bifurcation curve in Fig. 4(b) shows the periodic and chaotic regime of DW in phase space with respect to magnitude of current density.

2) 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, 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. Fig. 5 represents the stochastic nature of notch location with respect to shift pulse. The DW with same initial velocity simulated with two different shift pulse characteristics (with same average value) moves with different velocities. The DW speed and polarity are also related to the type of wall-antivortex (AV), vortex (V), and transverse (T). AV wall is typically metastable and possesses bi-directional motion. Once converted to V or T, it shows an increase in speed and uni-directionality. Therefore, DW velocity is stochastic in nature.

3) Stochastic DW pinning: The DW moves smoothly if the nanowire (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 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 particle trapped in a potential well. The depinning is also a stochastic process and depends on injected current magnitude, frequency and environmental conditions. Fig. 5(b) represents the stochastic nature pinning due to notch location, DW speed and shift pulse. Fig. 5(c) shows that an out-of-sync pulse may degrade the DW speed and lead into pinning.

4) Stochastic DW annihilation: Two DWs can annihilate each other due to a) oscillatory motion under the influence of injected shift current; b) slight difference in velocities due to stochastic nature of DW motion; and c) metastability of the walls and resulting change in polarity of DW motion.

5) Nonvolatility and retention time: The DWs retain their state in absence of external assistance. The retention time is a function of thermal stability of the DWs.

Macroscopic Properties:

1) 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 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.

2) Magnetic polarity dependent retention: The DWs retain their state in absence of external assistance. The retention time is a function of thermal stability of the DWs. Long retention could be useful for tamper detection sensors.

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

4) 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 number of bits per NW is set by the NW dimensions.

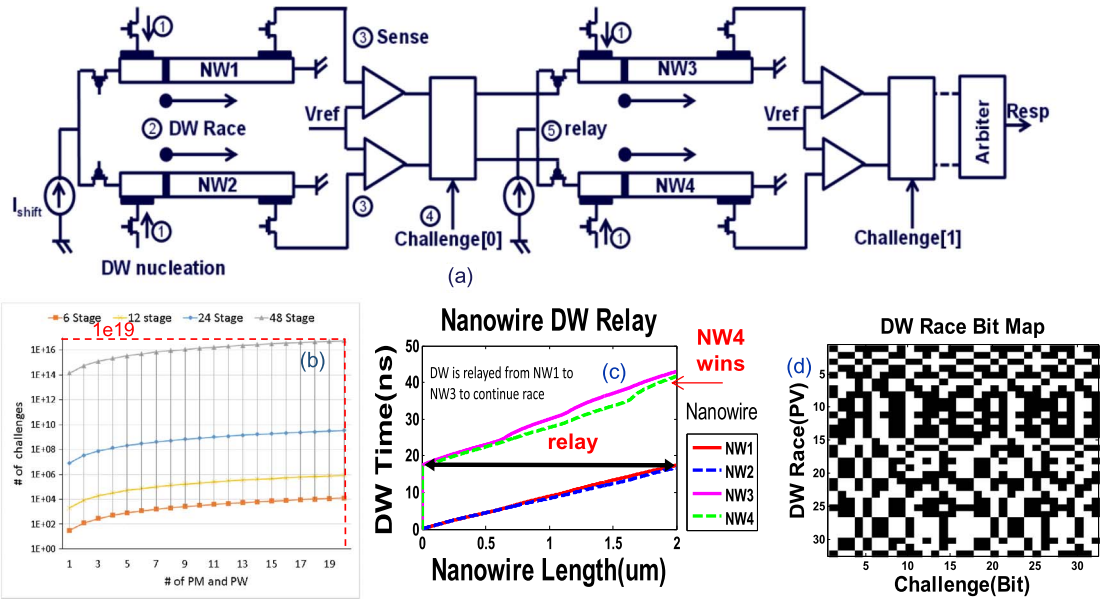

Fig. 6. *(a) Schematic of DW relay-PUF. I_{shift} pulse magnitude and width can also be used as challenges. Sequence of events is numbered from 1 to 5. (b) # of challenges wrt # of relay-PUF stages, PM & PW. With 48 stages and 20 PM/PW settings total # of challenges= 1e19, i.e., ten years simulation time. (c) Simulation showing relay race and winning DW. (d) PUF response under variations [153], [154].*

5) 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.
6) Miscellaneous properties: DWM provides opportunity to exploit multiple sense points (read heads) along the NW for continuous collection of entropy and randomness.

III. SPINTRONIC SECURITY PRIMITIVES

The previous section covers the basics of hardware security primitives, various flavors of spintronic elements and their security-specific properties. This section presents the design of spintronic hardware security primitives and interesting features offered by them.

A. Physically Unclonable Function (PUF)

1) DWM PUF:

A. Design and Operation: In [153]–[155], the physical randomness in the DWM is employed to generate response for a challenge. Fig. 6(a) illustrates a relay-PUF design with series connected NW stages. The conventional muxing circuit between each stage is introduced to toggle paths and create new challenges. More number of stages also provides 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.

1) 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. Fig. 6(b) shows that obtaining the same number of challenges will require significant area and power overhead. With $1e^{19}$ challenges, it will take approximately ~10 years to decode the response by an adversary, making the PUF attack-resistant.
2) 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 Fig. 7(a). Next, the shift signal of stage-1 is activated, that 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

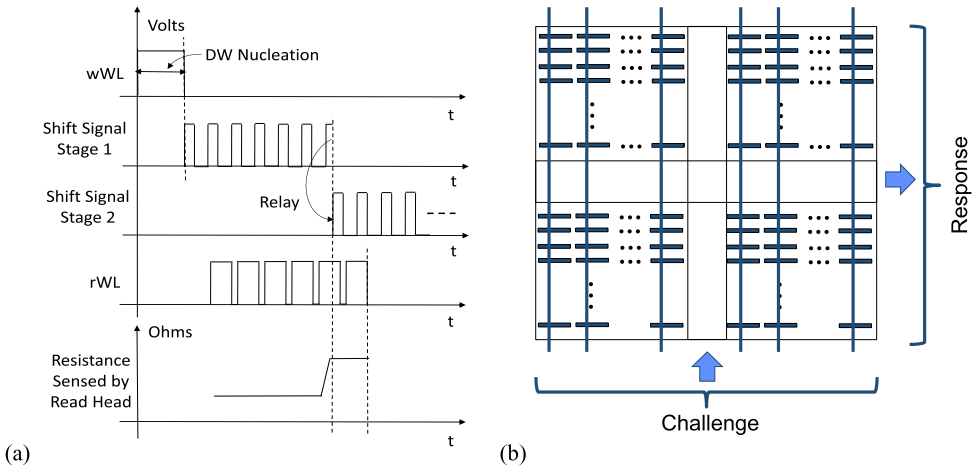

Fig. 7. *(a) Timing diagram showing the write and read wordlines and the shift signals for each stage and, the resistance sensed with respect to time. (b) Schematic of memory-PUF [153], [154].*

head detects the arrival of the DW (the DW reaches the end of 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.

3) 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.

In addition to the relay-PUF, a memory-PUF is also proposed [153] 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 shown to be low-power compared to SRAM PUF. The schematic of memory-PUF is shown in Fig. 7(b).

B. Evaluation of DWM PUF [153]: The DWM PUFs are evaluated with respect to quality metrics such as strength, randomness, and repeatability as described below.

Strength: The DWM 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 additional set of challenges. Therefore, the relay-PUF could be categorized as a strong PUF whereas the memory-PUF could be categorized as a weak 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.

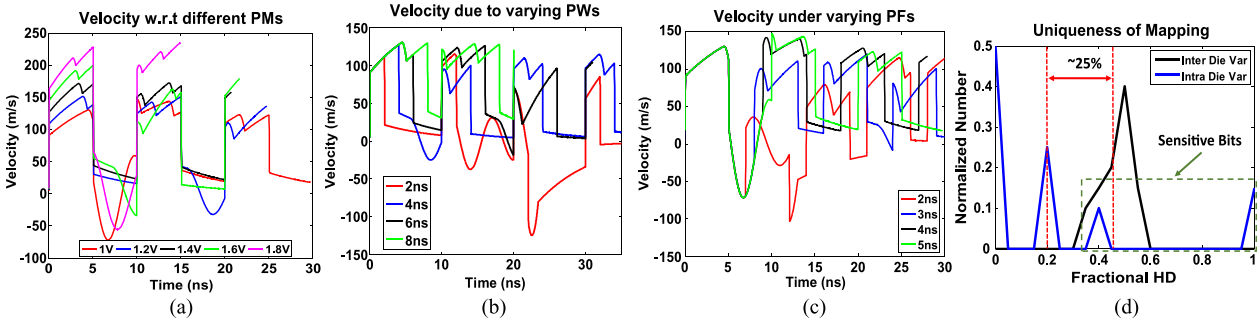

Fig. 8. *Relationship of DW velocity on the three pulsed voltage conditions [153] (a) for various pulse magnitude (PMs), (b) for different pulse widths (PWs), (c) for different (pulse frequencies) PFs (legend shows the off-on time = 5 ns, pulse period for (a) and (b) is 10 ns), and (d) inter and intra-die HD distribution.*

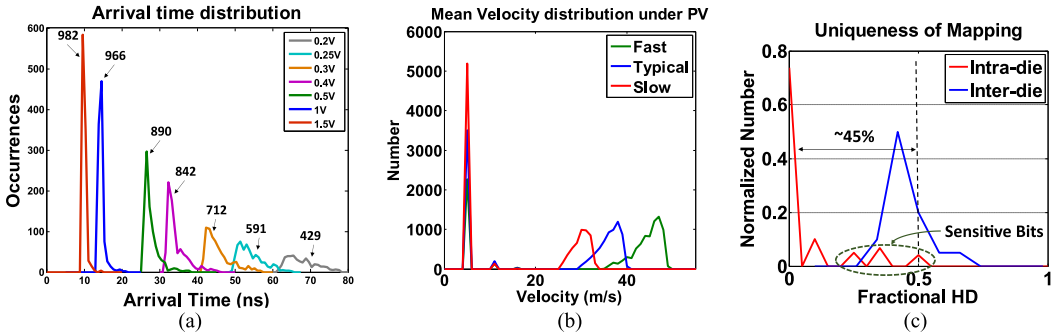

Fig. 9. *Arrival time distribution [153] for (a) different shift voltage settings at 25 °C, (b) velocity distribution in the memory array for fast, slow, and typical corners, and (c) inter-and intra-die HD distribution for memory-PUF.*

The behavior of the DW in response to shift current pulse magnitude, width and frequency is illustrated in Fig. 8(a)–(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 PUF resilient to modeling and machine learning attack [155].

Randomness and Stability: For simulation a six-stage PUF at 25 °C and 0.25 V is considered. The DW dynamics in the NW is solved by using stochastic 1D-LLG [159]. Fig. 6(c) shows the DW race in two NWs with respect to time. Fig. 6(d) 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 intra-die HD, the PUF response is compared by considering two extreme operating temperatures −10 °C and 90 °C, and voltage variations of ±10%. A long tail in the distribution is obtained due to sensitive bits that are highly susceptible towards temperature and voltage variations [as seen in Fig. 8(d)]. In order to ensure low intra-die variation, additional techniques have been suggested [153] such as: 1) temporal redundancy where the response of the bit is observed at different time instances and majority response is used as the final output, and 2) error correction circuitry such as Von-Neuman corrector [66] and run length encoding [119] to fix the unstable bits. An average of 25% separation between the inter-die and the intra-die variation is observed for relay-PUF which shows good randomness and stability.

For memory PUF, 100x100 array per PUF is assumed [153]. For HD analysis, the notch dimensions for the inter-die process variations are varied according to a Gaussian distribution. The operating voltage is determined to ensure equal distribution of "1" and "0." The simulation at 1 V shift pulse shows that only 34 out of 1000 NWs get the DWs pinned [Fig. 9(a)]. In order to balance the "0" and "1," the shift pulse voltage is reduced. It is noted that shifting at 0.25 V roughly produces 59% of "1" (i.e., the DWs that win the race). By operating the memory-PUF at this voltage [Fig. 9(b)], it is ensured 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 fixed time (after 100 ns for instance). The average inter-HD is found to be 50%. An average of 45% separation between the inter-die and the intra-HD is observed for memory-PUF.

Area and power: It has been noted in [153] that the DW memory-PUF is 10x more power-efficient than SRAM-PUF when the number of sense points are increased to 8 (Fig. 10). The footprint is found to be better by an order of magnitude.

2) STTRAM and MRAM PUF: In [12], a STTRAM PUF is proposed that exploits the randomly initialized free layer of STTRAM to generate a response. The technique compares two STTRAM bits from complementary rows during registration phase to generate a response. In case of bits that are initialized to the same value during comparison, the technique relies on the noise and sense amplifier offset to decide the response. To ensure repeatability, the PUF writes back the complementary

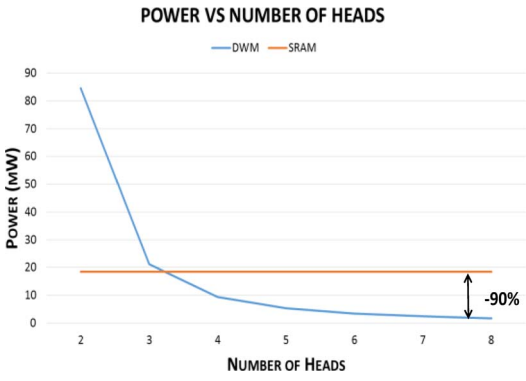

Fig. 10. *Reduction in power with respect to increase in number of heads for fixed number of challenges.*

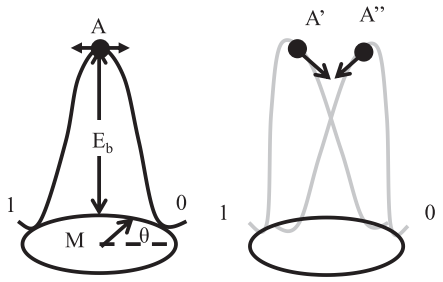

Fig. 11. *Energy landscape of MTJ for (a) perfect geometry and (b) random variations in cell geometries which causes the magnetization at location A to develop a preferential initial state.*

values on the MTJs. A fuzzy extractor is used to enhance the quality of the PUF response further. The random initialization of the MTJs make the PUF response highly entropic whereas its nonvolatility after writeback preserves the PUF response over multiple accesses and voltage and temperature fluctuations. The PUF [12] ensures a bit error rate (BER) of $\sim 10^{-6}$ from retention and read/write errors after writeback. The entropy attained by the PUF is 0.985.

Another work [13] describes MRAM PUF which employs the random initialization of the MTJ due to physical variations in the MTJ. The variations create random tilt of energy barrier as shown in Fig. 11. The distribution of tilt angle is Gaussian. Therefore, the MTJ free layer is prone to prefer certain initial orientation much similar to SRAM PUF. The technique first destabilizes the MTJ to the hard axis and releases it to settle to its preferred state. Exercising NIST benchmarks [135] on the PUF response demonstrate intra-die HD of 0.0225 and an entropy of 0.99. Techniques such as decreasing the aspect ratio at constant volume and increasing the volume at constant aspect ratio have been proposed to increase the tilt angle variation and enhance the stability of the PUF.

Design challenges: The stability of STTRAM and MRAM PUF during normal operation can be affected by factors such as the following.

1) Thermal noise: The noise can lower the retention time of the MTJ. This effect is more pronounced at higher temperature. Therefore, the PUF response will differ from registration value resulting in poor intra-HD.
2) Read disturb: Multiple read of a bit can cause read disturb which will flip the bits resulting in poor intra-HD.
3) Write failure: If the PUF involves write operation e.g., writeback in [12], failure to write the desired value can cause poor robustness.
4) Reliability/endurance: Multiple write operation can lower the lifetime of the MTJ (due to oxide breakdown), resulting in a bit that could be stuck at 0 or 1.
5) Tampering and side channel attacks: Temperature and magnetic field can be employed by an adversary to write or modulate the state of the PUF array. The objective of the attacker could be to gain insights for modeling the PUF responses and/or to bypass the authentication. It has been noted that the effect of magnetic tampering is expected to be low due to inherent resilience of scaled STTRAM from magnetic field however temperature could be used to tamper with the retention time of the PUF [156].

B. Encryption Engines

The DW properties such as shift-based access and dependence of MTJ resistance on relative orientation of the free layer and fixed layer can be employed to realize

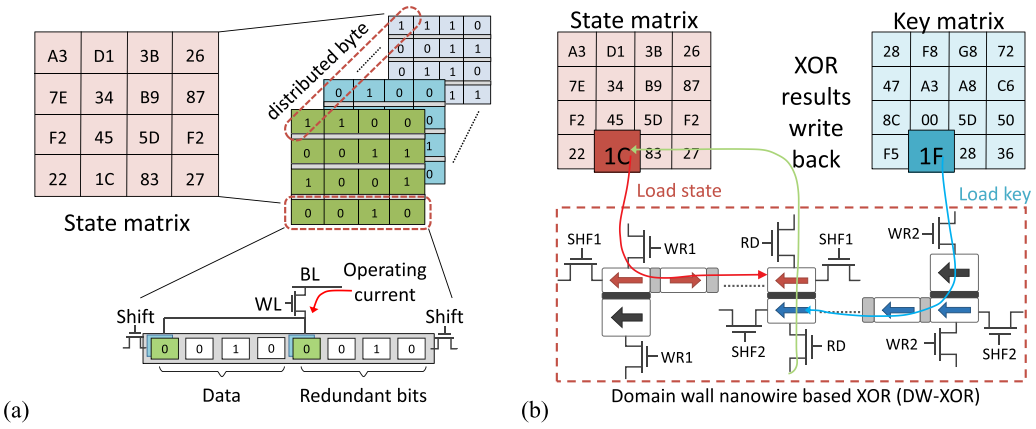

Fig. 12. *(a) Data organization of state matrix on domain-wall nanowire [14]. (b) AddRoundKey step using domain-wall-based XOR gate [14].*

encryption engines. AES is a standard encryption algorithm that has been investigated in [14] using DWM. Due to dominant shift and XOR operations AES is inherently suitable for DWM's serial access architecture. Superior energy efficiency, entropy, and density of DWM-AES is promising for encryption engines. Each AES step is mapped to a corresponding DWM operation. The basic building block is a 2-input XOR gate that is realized by shifting the input bits in two nanowires that are built on top of each other [Fig. 12(b)].

To start the AES operation, first the state matrix is implemented in the DWM array, as shown in Fig. 12(a). Each byte of SM is written across eight nanowires to enable cycle-by-cycle AES operation. The following approach is adopted to perform the AES steps using DWM.

- Step 1) SubByte: In this step, each byte of SM is replaced using the same substitution function. A DW-based look-up table (LUT) is used to save leakage power of conventional SRAM-based LUT.
- Step 2) ShiftRows: This operation rotates each row cyclically to the left by the amount equal to the row number. To mimic cyclic rotation in nanowire, redundant bits are employed in DW nanowire where the bits are repeated. This is shown in Fig. 12(a) where the data bits 4'b0010 is repeated again. Therefore, simple left-shifting of bits mimic the rotation operation.
- Step 3) MixColumns: This step maps each column of the SM to a new column by multiplying it by a matrix containing numbers 1, 2, and 3. These operations could be achieved by shift and add. The shift operation is natural in DWM therefore multiplication is achieved by shift and addition. For addition, the domain-wall XOR gate is employed as shown in Fig. 12(b).
- Step 4) AddRoundKey: This step XORs the SM with the round key. DW-XOR is utilized in this step as shown in Fig. 12(b).

The DWM AES implementation [14] consumes 24 pJ/bit and provides a peak bandwidth of 5.6 GB/s. It is shown to be significantly efficient than CMOS and CMOS/molecular (CMOL) memristive implementation.

Design challenges: The functionality of DWM AES can be affected by factors such as the following.

1) Process variations: The process variation in magnetic nanowire can create surface roughness which can affect the shift operation. Similarly, variation in read/write head such as oxide thickness, surface area, TMR, saturation magnetization can affect the read/write operation. The variations can also alter the energy barrier lowering the retention time of the read/write head.
2) Read/write/shift/retention failures: The process variation in read/write MTJ can cause read and write failures during the AES operation. The shift failure during shiftrows and mixcolumns can also result in wrong computation. The volatility of the bits due to poor retention will also cause functional failures during AES computation.
3) Reliability/endurance: Multiple write operation can lower the lifetime of the MTJ resulting in a bit that could be stuck-at 0 or 1.
4) Side channel attacks: Temperature and magnetic field can be employed by an adversary to write or modulate the state of the DWM LUT and/or affect other operations. The objective of the attacker could be to weaken the security.

More research is required in this direction to understand the above challenges and develop countermeasures.

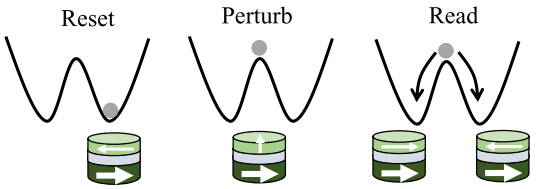

Fig. 13. ***Operating principle of TRNG using MTJ.***

C. True Random Number Generator (TRNG)

The chaotic phenomena of MTJ has been exploited to generate true random numbers. In [15], a spintronic dice is proposed where the key idea is to first reset the MTJ to AP state and next excite the free layer of the MTJ to the bifurcation point by applying a current pulse and let the magnetization settle in the random state due to thermal noise (Fig. 13). To improve the randomness of the response and kill the correlation among bits they are XOR'ed with each other. Although promising, the reset pulse is detrimental to MTJ reliability. Furthermore, the sharing of reset and sense circuit makes sense MTJ susceptible to read disturb.

A conditional perturb technique is proposed in [16] which avoids the usage of reset pulse by applying an optimal pulse and bring the MTJ to 50% switching probability contour. Therefore, a high-quality key generation is realized at lower energy and faster rate. Elimination of reset pulse also prolongs the MTJ lifetime. A complementary polarized MTJ structure is proposed to enhance the randomness of bits generated [17]. The precession of MTJ free layer is also employed to generate random number [18]. The current pulse width is applied and adjusted to cause the free layer precession that settles to a random state. A similar technique applies a current in between read and write current to the MTJ to change its

switching probability between 0 and 1. The random bit is extracted and processed further for key generation [19]. In [20], the MTJ is disturbed using DC current and the random value is sensed and processed using an entropy extractor. A tamper detection unit is also designed by monitoring a run of 0 s or 1 s in the random number generated from the MTJ array. Other MTJ-based TRNGs have also been proposed [173], [174].

Design challenges: The operation of STTRAM TRNG can be affected by factors such as the following.

1) Thermal noise: The noise can lower the retention time of the MTJ. This can add on top of the process variation induced poor retention of certain bits to make the response predictable. Therefore, the entropy of the TRNG can be lowered.
2) Read failure: Read operation can fail due to poor TMR/sense margin. This can weaken the TRNG since the response of certain bits could be predictable.
3) Write failure: The TRNG that involves write operation (e.g., RESET in [13]) can experience failure to write the desired value resulting in degraded entropy.
4) Reliability/endurance: Periodic write operation can lower the lifetime of the MTJ resulting in a bit that could be stuck-at 0 or 1 degrading the entropy of TRNG.
5) Tampering and side channel attacks: Temperature, magnetic field and other side channels can be employed by an adversary to write or read during AES operation. The objective of the attacker could be to gain clues about the key and intermediate data to weaken or crack the authentication.

IV. SECURITY VULNERABILITIES AND ATTACK MODELS

In the previous section, we explored the prospects of spintronics to enhance the security and trustworthiness of the designs. Here, we present the fundamental security vulnerabilities present in spintronic devices and describe the attack models to tamper with the content. Although the discussion is focused on STTRAM, similar attacks are also feasible on DWM and MRAM. Furthermore, different knobs for tampering such as temperature can also be exploited in addition to magnetic tampering that is described in this paper.

A. Fundamental Security Vulnerabilities

Sensitivity to magnetic field: In STTRAM the writing of MTJ is done using spin transfer torque (STT) term (for low power consumption) and external field H_a is kept 0 [see (1)]. However, external magnetic field can also be used to toggle the magnetization in absence of charge current (Fig. 2). Note that magnetic field-based toggling is the foundation of MRAM [167]. The attacker can exploit this extra knob to corrupt the free layer data. Both permanent magnet as well as electromagnet could be used for tampering by the adversary [158]. Similar issue persists for the read/write heads and magnetic nanowire of the DWM where the data can be tampered using external magnetic field.

Sensitivity to temperature: The magnetic parameters of MTJ are functions of ambient temperature (Table 2). The temperature modulation manifests itself in terms of functionality (read/write speed) and retention. Therefore, the adversary can employ this knob to tamper with the functionality or data persistence for information theft. The DWM heads have similar sensitivity to temperature.

Other tampering knobs: Localized laser-induced heating has also been employed for magnetization reversal as an alternative means to perform efficient write operations [21], [22]. A knowledgeable adversary can exploit this knob to tamper the bits (to cause functional failures) or steal the information. X-ray, radio frequency, and mechanical stress can also affect the magnetization dynamics of MTJ (in STTRAM, MRAM, and read/write heads of DWM) can be exploited for tampering.

B. Attack Models

The adversary can tamper the chip through an external magnet. The attack could be launched either through static (DC) magnetic field or alternating (AC) magnetic

Table 2 Temperature Dependency of MTJ Parameters for Vulnerability Analysis

Parameters	Model	Definitions
Retention [174]	$\tau = \tau_0 \exp(\Delta)$ where $\Delta = \frac{H_k M_s(T) V}{2 k_B T}$	H_k: anisotropy field, $M_s(T)$: saturation magnetization, V: free layer volume
Saturation magnetization (M_S) [175-176]	$M_s(T) = M_{s0}(1 - T/T_c)^{\beta}$	M_{s0}: saturation magnetization at 0K, T_c: Curie temperature, β: material dependent constant
Polarization (P) [177]	$P(T) = P_0\left(1 - \alpha_{sp} T^{\frac{3}{2}}\right)$	P_0: Polarization at 0K, α_{sp}: Geometric constant
Conductance (G) [176]	$G(\theta) = G_T\{1 + P^2 cos\theta\} + G_{SI0} T^{\frac{4}{3}}$	$G_T(G_{SI0})$: Conductance due to direct elastic tunneling (imperfection effect), θ: tilt angle
$TMR(T) = \frac{TMR_0(T)}{1+(V/V_0)^2}$ [178]	$TMR_0(T) = \frac{2P_0^2\left(1-\alpha_{sp}T^{\frac{3}{2}}\right)^2}{1-P_0^2\left(1-\alpha_{sp}T^{\frac{3}{2}}\right)^2 + \frac{G_{SI}(T)}{G_T(T)}}$	V_0: voltage at which TMR is halved.

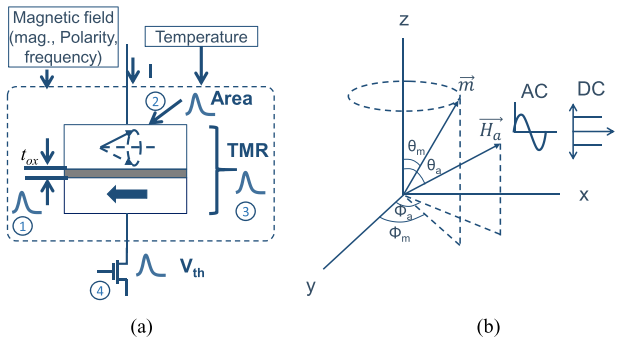

Fig. 14. *(a) STTRAM bitcell with various sources of process variations and tampering parameters. (b) Free layer magnetization in polar co-ordinates (θ_m and Φ_m). The attack field (H_a) in polar co-ordinates (θ_a and Φ_a) and type of attack (AC, DC) is also shown.*

Table 3 MTJ Parameters

Parameter	Value
Dimension	60nmx120nmx3nm
Damping const (α)	0.01
Sat. Mag. (Ms)	1000 A/m
Exchange Constant (A)	2e-11 J/m.
Polarization	0.8
Spin conductance	1e-3
Activation energy (E_a)	56kT
Anisotropy const (Ku)	E_a/volume

field [158]. In DC attack the applied field is unipolar, but the magnitude can be changed. The AC field can be applied with varied characteristics such as frequency, magnitude and shape. Both DC and AC fields can be applied in certain direction in 3-D space. The STTRAM bitcell and the attack on free layer are shown in Fig. 14(a) and (b).

DC magnetic attack [158]: The polarity of DC attack is fixed in time. Therefore, it can only create data-dependent unipolar failures. Note that the free layer polarity is data dependent. The direction of applied field could be same or opposite of free layer orientation. If they are opposite, the field creates *retention failures*. If they are in same direction, the attack only increases the retention time which will not cause any functional failures. During write operation a field in same direction prevents the flipping of the magnetization which in turn results in either hard or soft *write failures*. The hard failure occurs when the bit fails to toggle even with infinitely slow write operation. The soft failure results in increased delay in write which can be potentially mitigated by slowing down the clock frequency [192]. The opposite field direction assists the bit flipping which speeds up the write operation. In all of the above scenarios a larger magnitude of applied field accentuates the read, write and retention failures. The tilt angle of the applied field in 3-D space also modulates the failure behavior.

AC magnetic attack: Switching of MTJ using AC magnetic field and current by exploiting the resonance dynamics of free layer has been explored for energy-efficiency [188], [189]. It has been noted [158] that AC field can also be exploited by an adversary to tamper with the bits. In this scenario the resonance dynamics of free layer can aid the adversary in tampering. AC attack is more detrimental as it affects both storage polarities (depending on the frequency of applied field with respect to read and write speed or time between successive access to a bit). If the field frequency is faster than two successive accesses to a bit then it may cause retention failure regardless of storage data polarity. This is true because the applied field will change polarity while the bit is still in retention. A faster frequency also perturbs the free layer magnetization more and increases the flipping probability during retention.

The similar logic applies to write failure as well. During write operation, the AC field assists the write during the phase when the field is opposite to the storage polarity and resists the write in the phase when they are in same direction. Therefore, if the frequency of external field is higher than write frequency (i.e., inverse of write time) then both storage polarity (i.e., all bits that are being written) gets affected. At slower attack frequency only one storage polarity is affected among the bits that are being written. Note that even with the slow frequency if the magnetic field is transitioning from positive to negative or vice versa, both storage polarities are affected (although the magnitude of the field could be relatively small). Similar to DC field, a larger magnitude of AC field accentuates the write and retention failures. The tilt angle of the applied field in 3-D space also modulates the failure behavior.

C. Attack Analysis

For attack analysis an in-plane MTJ with parameters shown in Table 3 is employed [158]. It can be noted from Fig. 15(a) that the MTJ polarity could be flipped in retention mode for fields greater than 220Oe. The flip time reduces with increasing strength of the magnetic field. The comparison of MTJ stability between retention and functional mode (with read and write currents) is considered in Fig. 15(b) and (c). For the analysis different magnitudes of read/write currents and polarities are assumed. It can be observed that the bits fail easily when the current polarity and magnetic field are in the same direction (assistive). The flip time is higher when current and magnetic field are in opposite direction (suppressive). Note that the read corresponds to 50 uA current and 100–250 uA corresponds to the write operation. Magnetization reversal time with 50-uA current essentially indicates the read disturb.

The impact of AC field on retention stability is plotted in Fig. 15(d). It can be observed that higher

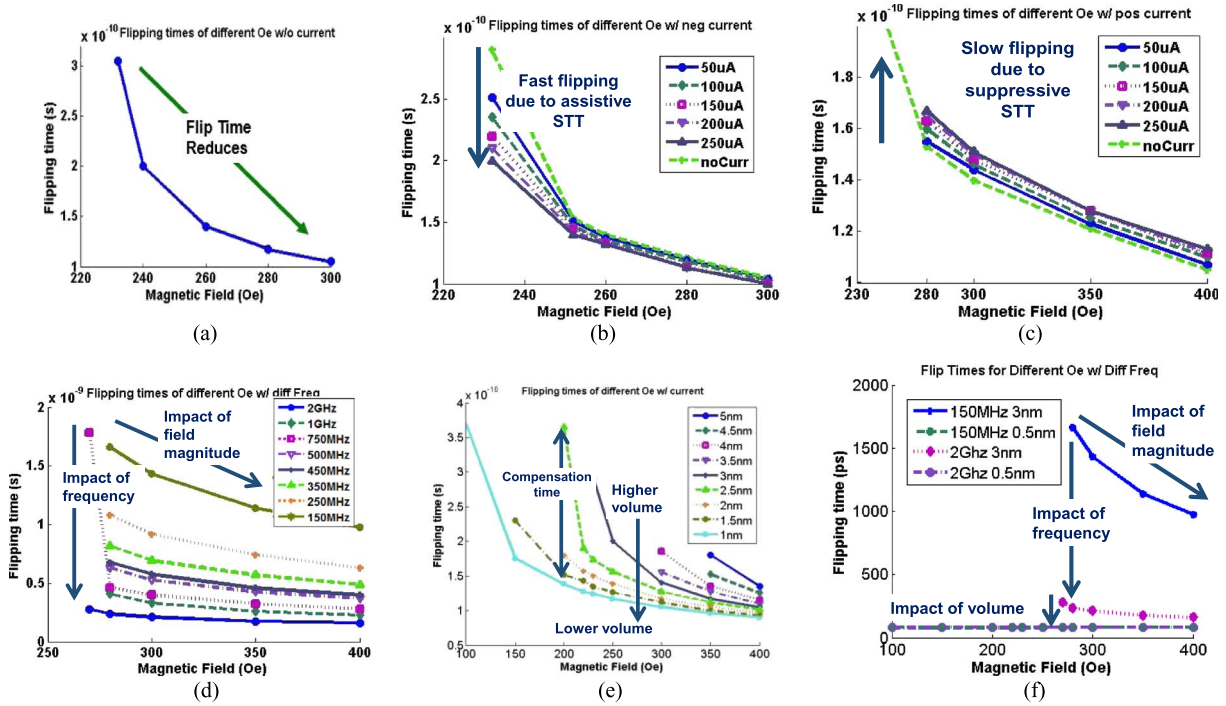

Fig. 15. *Impact of DC magnetic field on the stability of free-layer [158]: the impact of flipping time with (a) magnetic field strength for bits in retention, (b) assistive current during write, and (c) suppressing current during write. (d) Impact of AC magnetic field on the stability of free-layer. (e) and (f) Impact of MTJ volume on the flip time in presence of DC and AC magnetic fields, respectively. Results are obtained using OOMMF [148].*

frequency magnetic field can cause more damage even with smaller amplitude than lower frequency magnetic field and higher amplitude. This is primarily due to the fact that high frequency field creates more noise in the magnetization dynamics. Interestingly, the frequency of attack field is more damaging than its strength. Therefore, the adversary can potentially increase the impact of attack by using weak but high frequency magnetic field.

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. Fig. 15(e) 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). The simulation results for AC attack [Fig. 15(f)] indicate that higher volume can protect against attack of lower frequency. High-frequency attack can cause failure regardless of MTJ volume.

Note that although [158] focuses on in-plane magnetization anisotropy (IMA) STTRAM the community is devoting significant research effort on perpendicular magnetization anisotropy (PMA) STTRAM which is potentially more scalable and energy efficient [187]. Due to higher magnetic anisotropy PMA STTRAM is also expected to be more robust to magnetic attack. More research is required to understand the viability and impact of magnetic attack on various flavors of spintronic devices.

D. Impact of Process Variation

Fig. 16(a) and (b) shows the mean and sigma of flip time for different strength of DC magnetic field. An assistive current of 0–500 uA is considered. It can be noted that mean flip time reduces due to more disturbance. Interestingly, the sigma increases because the process variations in MTJ and access transistor modulates the current which in turn affects the flip time. This plot also indicates that the bitcells are more robust to attack in retention mode (0 uA current) regardless of variability. The functional mode amplifies the impact of variability and results in random bit errors.

V. SENSING AND MITIGATION

In the previous section we described security vulnerabilities and attack models. This section is focused on attack sensing and mitigation. Note that although the discussion is limited to magnetic attack, other types of sensors and prevention techniques are also possible and requires equally important considerations.

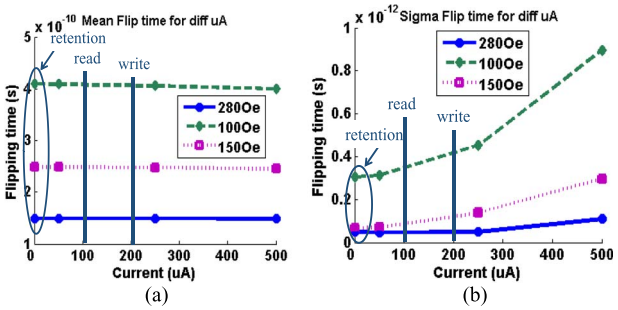

Fig. 16. *Impact of process variations on flip time during retention and functional mode (a) mean; and, (b) sigma [158].*

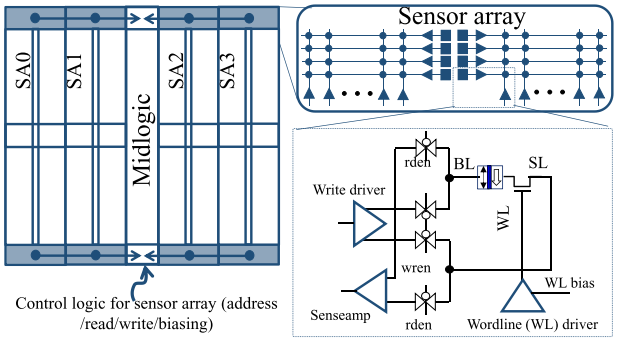

Fig. 17. *Embedded attack sensor in memory array [158]. The details of sensor array with peripheral circuits is shown in inset. Control logic is shared among the subarrays and contains the logic to generate address, read, write, and data and analyze the response.*

A. Sensing Magnetic Attack

The key objective of the sensor is to sense or detect magnetic field attack "proactively" in order to trigger corrective steps for the functional STTRAM array. Therefore, the sensor can avoid wrong operation of memory under magnetic field attacks through compensation and appropriate error correction that tailors the error correction capability to the intensity of the external magnetic field. The sensor should be able to sense an attack ahead of time, i.e., before the memory corruption. It can also sense: 1) the intensity of the attack; and 2) the polarity of the attack, both of which can be useful in auto-protecting a memory subsystem against data corruption.

In [158], a small replica of the STTRAM array is proposed as a sensor. Although functionally equivalent to the actual array, the sensor is designed to meet the objectives described above. The sensor is embedded in the array (in the peripheral areas) to capture the spatial variation in magnetic attack (Fig. 17). It can be observed that restricting the sensors to peripheral areas might provide opportunity to attackers to a tamper with the bitcell area through carefully orchestrated magnetic field. One possible solution is to distribute the sensors in every transition region of subarray including the interface between wordline driver-to-array, column-to-array, and array-to-array. The transition region is repeated significantly in memory array leaving very small fraction of pure bitcell area exposed to attack. Targeting such small regions using a commercial magnet could be extremely hard. The sensor array is designed by modifying the actual STTRAM array. The intensity of the attack is sensed through the error rate of the sensor array. High error rate corresponds to higher intensity. The sensors have the following salient features to quantify the intensity and polarity of attack [158].

1) *Multiple copies with different free layer volumes*: Multiple copies of sensor each with different MTJ free layer volumes e.g., small and medium will be employed. The objective of changing the MTJ sizes is to sense the attack even in presence of process variation.
2) *Distribution of sensors*: These different flavors of sensors can be distributed in the cache to collect the spatial responses.
3) *Weak writing/stress*: From (2), if a small amount of current is injected into the MTJ, the thermal energy barrier is lowered. Therefore it is possible to inject weak current in sensor STTRAM array so that it fails early (since retention time is $T_{\text{ret}} = f_0 * e^{\Delta}$ where f_o is the thermal attempt frequency, which is roughly 1 GHz). The weak writing could be accommodated by using design-for-test (DFT) circuit to keep the write drivers active and bias the wordline voltages appropriately to tune the bitcell current (Fig. 17). The column multiplexers are kept ON to enable weak writing of all columns.
4) *Array architecture*: The sensor array is always kept ON (during functional and retention mode) to sense the attack. The total number of global columns is kept 1 to lower area, power overhead (especially for weak write sensors) and faster test time. The column area contains sense amplifier and write driver and row area contains minimal sizes wordline driver that is modified to provide biased voltages to access transistors.
5) *Data polarity*: Different data polarities could be stored in the sensor array to detect the direction of attack. One example is to store block 1's (0's) in the sensor to detect DC attack in negative (positive) direction. Block 1 and 0 pattern will capture unidirectional fails. Checkerboard pattern could be stored to detect AC attack (to capture bidirectional fails).

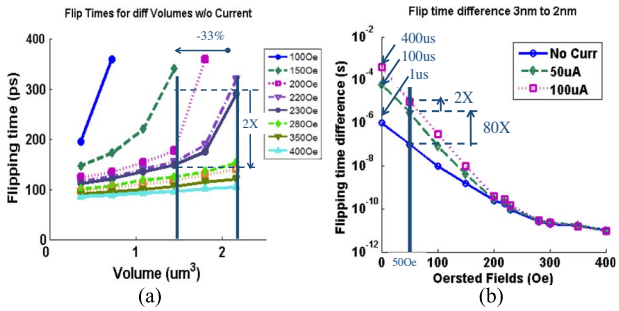

Fig. 18. *Sensitivity free layer volume on flip time [158]: (a) 33% reduction in volume reduces flip time by 2x and (b) effectives of volume scaling and weak write on early detection of attack. Reduction of 33% volume can detect 50Oe attack ∼100 ns before actual array fails. Weak write of 50 uA can provide 80x more time. An additional 50 uA can provide 2x extra time.*

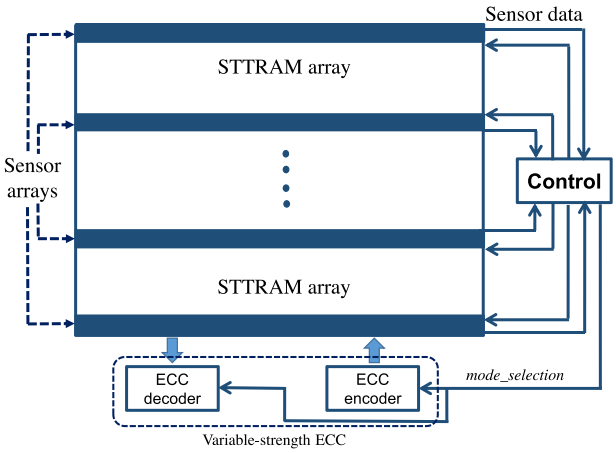

Fig. 19. *Overall system protection approach that includes an STTRAM array with embedded sensors, attack mitigation, and variable-strength ECC [158].*

6) *Test speed and compensation window*: The test is executed in parallel with stressing of neighboring sensor arrays (for weak write sensors). For test, first the stressing of the array and weak assertion of wordline is paused. Next, read followed by write is performed to reinitialize the bits. The error rate determines the magnitude of attack. The test speed determines the amount of time left for launching the compensation. For example, if the bits fail ∼100 ns before the real bits and test takes 25 ns then the time available to enable mitigation techniques (which is compensation window) is 75 ns. Fig. 18(b) shows that a sensor with 33% lower volume can detect a 50Oe attack 100 ns before the real bits are corrupted. This window can be expanded further by adding weak write for proactive mitigation steps.
7) *Control logic*: The control logic resides in midlogic area and generates address, read/write signals and data and, collects responses to determine error rate from various sensor flavors (Fig. 17).
8) *Power saving*: Note that weak writing of bits may cause significant power overhead. To harness the benefit of early attack detection while lowering the power consumption, the sensors with weak write (sensor-w) could be: 1) interleaved with normal sensors (sensor-n); and 2) turned on periodically.

Fig. 18(a) and (b) shows the sensitivity of free layer volume with respect to the flip time of DC attack [158]. It can be noted that flip time is very sensitive to free layer volume for lower magnetic field attack. A 33% lower volume reduces the flip time by 2X (for 220Oe). For lower fields (< 200Oe) the sensitivity is exponential. The flip time difference between functional MTJs and sensor MTJs is plotted in Fig. 18(b). For lower fields the flip time difference is extrapolated. The sensor MTJ uses 33% lower volume (sensor-n). The results indicate that a 50Oe attack could be detected ∼100 ns before the real bits is corrupted. For weak attacks (< 10Oe) the sensor can detect it ∼1 us in advance. By adding 50 uA of current (for sensor-w), the sensitivity could be improved by approximately ∼80X at the cost of extra power overhead. An additional 50 uA can improve the sensitivity by an additional 2X.

From the above discussion, it is evident that volume modulation and weak writing can be effectively employed to create two flavors of sensor arrays. Additional sensor flavors can be created by lowering MTJ volume further and/or combining weak write. Assuming four local columns and 128 rows per sensor array, the weak writing could cause 25 mW power (at 1 V) for sensor-w. Therefore, sensor-w should be judiciously used (by limiting their number and frequency of usage). The area overhead of the proposed sensors are less than 1% since they are embedded in the transition region of the arrays.

B. Attack Compensation

Fig. 19 shows the top level schematic of the sensing and compensation methodology [158]. The attack could be DC as well as AC and the magnitude could vary temporally and spatially. To capture the spatial variation the sensors are distributed along the array. The temporal variation is captured using sensitive sensor-w and regular sensor-n. The error rate and failing polarities collected from sensors are provided to a control unit that triggers compensation techniques. Due to proactive sensing, the control unit can trigger precautionary measures to improve the array resilience against the tampering.

1) Array Sleep: It has been noted [158] that the STTRAM bits are more robust to attack in retention mode than functional mode of operation. Therefore, the

array can be put in retention mode till the attack subsides. Although simple, this technique may result in performance loss due to stall and may still experience attack induced corruption of bits. For further resilience, this technique can be combined with adaptive strength ECC to ensure strong encoding before the enabling sleep and correction after wake-up. Note that reading, encoding and writing the bits is associated with significant power overhead. Therefore, this technique should be combined with appropriate application where only the "important" segment of cache could be protected to ensure quality-of-service requirement.

2) Variable-Strength ECC: In [158], variable-strength ECC is used to correct failures in STTRAM due to magnetic tampering. The variable-strength ECC can provide variable error correction capability to STTRAM array based on the strength of magnetic field attack. It can dynamically change error correction capability to provide the right amount of error protection to individual memory blocks against failures. In order to enhance the multi-bit tolerance scheme, Bose–Chaudhuri–Hocquenghem (BCH) cyclic code is used with 128 bit data-length [158]. The variable-strength ECC offers four different error correction capabilities (1 b/2 b/4 b/8 b), and the correction capability can be automatically adapted based on the intensity/polarity of the magnetic attack measured in the tamper detection sensor. When there is no magnetic attack, ECC can be completely turned off or work with simplest ECC (1-b correction). As the magnitude of the attack becomes intense, the control unit in Fig. 20(a) can adapt ECC to provide stronger error corrections (2-b/4-b/8-b corrections). When smaller error correction options are selected, the unused modules in the ECC can be easily turned off to save computation energy.

1) *Variable-strength ECC encoder* [158]: BCH encoder is composed of two parts, Galois field adders and dividers. The division part is designed according to generate polynomial $g(x)$, and different error correction BCH encoders generally have different generator polynomial $g(x)$. Four different division parts are used in the reconfigurable encoder (1 b/2 b/4 b/8 b). The area overhead of the different division parts is small since the area of BCH encoder is much smaller (around 5%) than that of decoder.
2) *Variable-strength ECC decoder* [158]: The VC-ECC decoder is basically similar to 8-b correction BCH decoder. However, the architectures are designed scalable such that simple control logics can easily turn off the unused modules when the correction capability is 1 or 2 or 4 or 8 b.

First, the syndrome generator of the VC-ECC decoder is similar to that of 8-b correction BCH. As shown in Fig. 20 (b), since the syndrome generator for 1-, 2-, or 4-b correction BCH can be expressed as a subset of syndrome generator for 8-b correction BCH [23], the architecture is scalable, which means that only 12.5%, 25% or 50% of syndrome generators can be utilized with simple control logic to generate the syndromes for 1-, 2-, or 4-b correction BCH, respectively. Key equation solver (KES) and Chien search modules can be designed to be scalable like the syndrome generator, and the unused module can be simply turned off. The turning-off scheme applied to the syndrome generator are illustrated in Fig. 20(c). Simple pull-up and pull-down transistors with correct dimensions are being used based on whether the 1-, 2-, 4-, or 8-b correction scheme is being exercised. The pull-down NMOS transistor is required to ensure that the syndrome generator modules provide "zero" output when unused for correct ECC functionality. Details of the power-gate inclusion were obtained from [24].

Table 4 shows the implementation results of the variable-strength ECC decoder using 65-nm standard-cell

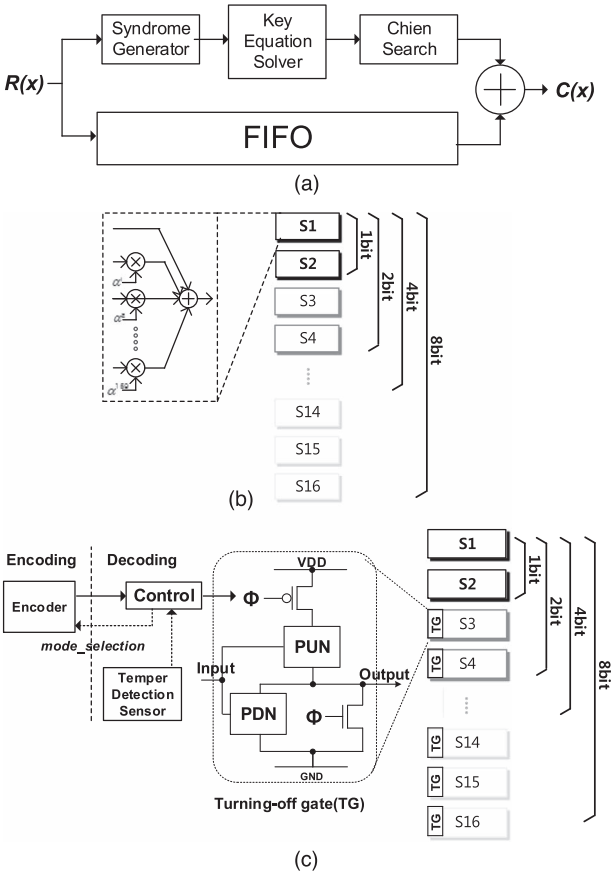

Fig. 20. ***Variable-strength ECC architecture [158] (a) BCH decoding process. (b) Example of scalable syndrome generator. (c) Dynamic reconfiguration scheme applied to syndrome generator using turning-off gate [25]. The turn-off signal Φ is generated from control module.***

Table 4 Hardware Implementation Results of Variable-Strength ECC [158]

BCH Type	1Bit Cor. BCH	2Bit Cor. BCH	4Bit Cor. BCH	8bit Cor. BCH	Reconfi. BCH
Total area (Gate counts)	6108	10298	18887	36557	37407
Critical path	6ns	6ns	6ns	6ns	6ns
# of Cycles	3	4	6	10	3/4/6/10
Parity bits	8	16	32	48	8/16/32/48
Power (mW)	1.62	2.46	3.87	6.21	1.78/2.55/4.13/6.35

CMOS library. Separate 1- (Hamming), 2-, 4-, and 8-b correction BCH decoders are also shown for comparison. As the error correction capability increases, the area requirement is understandably larger. The area overhead of the variable ECC is not significant compared to 8-b correction BCH decoder.

3) *Dynamic adaptation scheme* [158]: The variable-strength ECC has four choices of error correction capabilities, and the correction mode can be controlled using 2-b *mode selection* signal as shown in Figs. 19 and 20(c). This *mode selection* signal is generated from control logic, and the information is updated at runtime on a regular basis by monitoring the magnetic attack strength at tamper detection sensor. When the strength of attack becomes larger, the dynamic adaptation scheme can change *mode selection* signal to offer stronger error correction capabilities. For protection of on-chip cache memory, the 2-b *mode selection* is stored per cache block to indicate the encoding type, and the number of ways to store ECC bits is dynamically adjusted during runtime [25]. The 2-b overhead for the *mode selection* storage is negligible (< 0.3% area overhead) considering a typical cache block size (e.g., 512 b). If a block cannot be corrected due to inadequate correction capability, then its dirty bit is set and the data is fetched from the next level. For last level of memory, even higher protection may be needed. An alternative way of checking the occurrence of STTRAM failures is by ECC itself since the nonzero syndrome from the syndrome generator indicates memory failure occurrence. The syndrome monitoring scheme can be used to check the frequency of STTRAM failures in the functional mode [158].

Table 5 shows BER results when variable-strength ECC is applied to STTRAM cells which are under attack with various strength of magnetic fields. Input vector with 10^8 bit is used for the BER simulations. In the table, magnetic attack strength of 76.9Oe 100 μA means that 76.9Oe is combined with 100-μA current to model active operation mode. According to the results, when the magnetic attack strength of 76.8Oe 100 μA is used, STTRAM cells show raw BER of $3 * 10^{-3}$. In this case, ECC with 4-b corrections $(t = 4)$ can be selected to correct STTRAM bit failures. When the attack strength is as large as 76.9Oe 500 μA, the STTRAM raw BER is too large $(9.7 * 10^{-1})$ that the failures cannot be corrected even with 8-b correctable ECC. However, the adaptive ECC scheme using BCH codes can detect any number of failures by checking the output of the syndrome generator (i.e., all zero means no failure). If bit failures are detected which are too many to correct by the current ECC, then the corresponding cache blocks can be invalidated, thus preventing use of wrong data.

The information in Table 5 can be used for *array sleep* when the magnetic attack strength can be proactively determined. For example, when the predicted attack strength is around 76.7Oe 100 μA, the ECC correction capability (t) of the variable-strength ECC can be decided as $t = 2$. Then, the memory data are read out, re encoded to match the correction capability of ECC to the level of external field and written back to memory before the memory goes to mode sleep.

Table 5 BERs After Variable-Strength ECC is Applied to STTRAM Cells Attacked With Various Strengths of Magnetic Fields [158]

Magnetic attack strength	STTRAM raw BER	ECC correct. capability (t)	BER
76.9Oe 100μA	$2.19*10^{-1}$	t=8	can't correct
76.85Oe 100μA	$4.7*10^{-2}$	t=8	$2.8*10^{-3}$
76.82Oe 100μA	10^{-2}	t=8	$< 10^{-8}$
76.8Oe 100μA	$3*10^{-3}$	t=4	$< 10^{-8}$
76.7Oe 100μA	$< 10^{-3}$	t=2	$< 10^{-8}$
76.9Oe 200μA	$4.04*10^{-1}$	t=8	can't correct
76.8Oe 200μA	$3.5*10^{-3}$	t=4	$2.05*10^{-6}$
76.7Oe 200μA	$< 5*10^{-4}$	t=1	$< 10^{-8}$
76.9Oe 500μA	$9.7*10^{-1}$	t=8	can't correct
76.8Oe 500μA	$4*10^{-3}$	t=4	$< 10^{-8}$
76.7Oe 500μA	10^{-3}	t=1	$5.7*10^{-6}$

VI. PRIVACY ATTACK MODELS AND PREVENTION

In the previous section, we described data security vulnerabilities and attack models. This section presents data privacy attack models on STTRAM LLC and preventive solutions. The privacy attack models hold equally true for caches designed using other NVM technologies.

A. Preliminaries

Although promising, LLC designed using NVMs brings new security challenges [149] that were absent in their conventional volatile memory counterparts due to persistent data present in raw form. Although we focus only on spintronic memory technology, other NVMs such as ferroelectric RAM [168], memristor [136]–[139], resistive RAM (ReRAM) [144]–[147] and phase change RAM (PCRAM) also face similar privacy challenges. Two possible attack scenarios are possible [156]: 1) the user powers down the microprocessor with persistent raw (and sensitive) data present in the LLC, the adversary logs in, issues read instruction, and retrieves the data; and 2) the user powers down the micro-processor containing persistent raw data, the adversary removes the processor and steals the data through sophisticated probing. Note that the data privacy can be addressed to some extent by seminonvolatile memory (SNVM) which is similar to NVM but with very low retention time (e.g., 1 s instead of 1 yr). The retention time is intentionally lowered to improve latency and power. Additionally, it provides better privacy as the data vanishes after power is turned OFF. However, it has been noted that SNVM is not sufficient as the adversary can modulate data persistence using temperature [156]. Therefore, an erasure architecture is proposed in [156] to destroy the data irreversibly at power OFF. Since erasure could be power—intensive operation (and might need a backup battery under power failure attack), the residual charge present in power rail can be recycled. A canary circuit is proposed in [156] to track the MTJ write time under unregulated supply.

B. Qualitative Analysis of Data Privacy in LLC

In the following paragraphs, we present a qualitative analysis of data privacy issues in volatile and NVM memories that can be used as cache.

1) Volatile Memory: The volatile cache such as SRAM and eDRAM is inherently more secure as the data vanishes on power OFF. A tamper-sensing unit is embedded in memory and in the event of tampering, the power to the memory is turned off or even shorted to ground [150]. As an effect when the power is back ON, the SRAM is initialized to random states with no correlation to earlier stored value. Though data remanence effect may cause some bit cells to retain the data but vast majority of the data is lost when the power is turned OFF. Similar statement is true for eDRAM. Therefore, powering down is considered as a successful protection mechanism for the data privacy of volatile memory.

2) Nonvolatile Memory: NVM retains data even after power OFF. This provides instant-ON experience as the operating system and application software used by the system can be retained in an initialized and executable state within the NVM when the system is powered OFF. This feature can be useful when the NVM is used as main memory, but for the cache the data may not be needed after power OFF. The tamper sensing unit cannot be used for NV cache protection since powering OFF memory fails to erase the data. Encryption will cause significant performance loss due to high latency associated with encryption/decryption of each transaction. There is a need to find an energy-efficient way of handling the data privacy issue in NV cache with minimum loss in performance.

3) Seminonvolatile Memory: The typical retention time for STTRAM is ten years, however, such high retention time is not required for cache as the data is not required when the system is restarted or the virtual address space is changed. Instead the retention time can be lowered to improve the write latency and write energy [151]. The write energy can be lowered by reducing the thermal stability of the MTJ. The switching current (I) decreases linearly with the reduction in thermal barrier (Δ), which in turn decreases the retention. The retention time (t) is exponentially related to Δ [from (2)], which is proportional to MTJ free layer volume. Therefore, downsizing the free layer lowers the retention time providing fast write latency and lower write energy. It has been noted in [156] that lower retention is good from the data privacy standpoint as the data will be lost by the time adversary tries to get it. Therefore, SNVM can be used as first line of defense to protect the data. However, it has also been noted [156] that the retention time can be increased dramatically by freezing the chip. Thus, SNVM cannot be used in isolation to preserve data privacy.

C. Attack Models

The data in the nonvolatile LLC is assumed to be in raw format due to lack of encryption. Generally, the cache is either accessed by the CPU or by the main memory. Therefore both scenarios are considered, i.e., when the data can leave cache and move to CPU or main memory and become susceptible to stealth. Also, drop-in replacement of SRAM with STTRAM as LLC is assumed in terms of security features. In other words security features such as valid bit erasure after power ON and encryption of cache to main memory bus are assumed to be absent. The adversary is assumed to be capable of probing the data bus between cache and main memory.

1) CPU Side Attack Models: Two cases can be considered [156]:

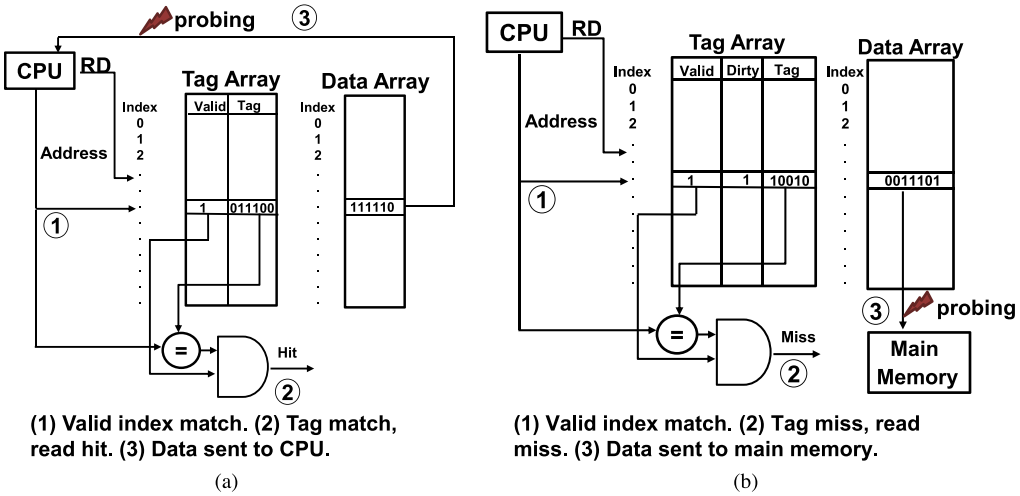

Fig. 21. ***Attack models and access sequence [156]: (a) read hit and (b) read miss. A direct mapped cache is assumed for these examples.***

1) Read Hit [Fig. 21(a)]: The CPU issues a read signal and the address is present in the cache (step 1), the corresponding valid bit can be found to be set indicating the data in the address is valid data. Thus, it produces a read hit (step 2) and the data from the data cache moves to the CPU (step 3). This is the easiest approach through which the adversary can retrieve raw user data from the last login.
2) Write Hit: This is not actually an attack, but it is just shown for the sake of completeness. Adversary can force a write signal and the address generated by the CPU matches both the index and tag resulting in write hit. Therefore the new data from the CPU overwrites the existing data. As the old data is overwritten, it cannot be obtained by the adversary.

2) Main Memory Side Attack Models: In this mode, the objective is to access the persistent data when it moves from LLC to main memory. The following cases are possible [156]:

1) Read Miss, Dirty = 1 [Fig. 21(b)]: Adversary forces a read signal and snoops the cache data when it is being replaced by the new data from the main memory. The address generated by the CPU matches one of the index (step 1) but the tag match fails and it results in read miss (step 2). The data in the cache needs to be replaced with new data from main memory, and if the corresponding dirty bit is "1" the existing data must be copied to the main memory. The data is thus accessible to the adversary who keeps snooping the bus between cache and main memory (step 3).
2) Write Miss, Dirty = 1, Write-Allocate: Adversary forces a write signal which results in write miss and tries to access the data when it is being replaced by new data from main memory [same as Fig. 21(b)]. The address generated by the CPU matches one of the valid index (step 1), but the tag match fails and it results in write miss (step 2). If the dirty bit is found to be "1" and the cache is assumed to follow write allocate policy, existing data in the cache must be copied to the main memory or victim cache and new data must be brought from main memory. Thus, the adversary can retrieve the data when it is being sent from cache to the main memory. In all of the above mode of attacks, the adversary can continue scanning through the address space of LLC and get as much data as possible.

3) Tamper Assisted Attack: In addition to noninvasive attacks discussed above that solely relies on changes of getting valid and/or dirty bit set, the adversary can deliberately alter the cache content through noninvasive tampering. The purpose is to set as many valid (or dirty) bits as possible to increase the chances of hit (or miss) and ease the attack. The following knobs can be used to tamper the bits [156]:

1) Magnetic Tampering: The cache memory can be exposed to external DC magnetic field in a direction that will flip the bits to "1". Note that this may also corrupt some of the data bits. However, small amounts of error in data can be tolerated and the original data can still be recovered [152] especially if the data is key value. The adversary can continue scanning through the address space of LLC after each round of tampering and get as much data as possible.

2) Thermal Tampering: In another form of tampering, the adversary can deliberately modulate the operating temperature with the intention to prolong the retention time to increase the number of persistent bits that can be compromised through unauthorized access at power-ON [152].
3) Miscellaneous Tampering: There are other tampering techniques [169] such as: 1) micro probing where conductors are attached to the chip surface directly to interfere with the integrated circuit; 2) radiation imprinting where the chip is exposed to X-ray radiation and the contents are burned in, so that power down or over write will fail to erase the contents; and 3) optical probing where a strong light/laser is shinned on the surface of the chip which turns ON the circuitry and if the circuit is ON, the parts that are active start glowing, assisting the adversary to determine the contents. Although not covered in this paper, the above tampering techniques can also be exploited by the attacker to steal persistent data in LLC.

D. Preventing Data Privacy Attacks

SNVM cache coupled with a low-cost, low-power architecture to erase the cache at power OFF is proposed [156] to ensure sufficient destruction of data that would prevent accurate reconstruction. Following paragraphs explain this approach.

1) SNVM Cache: SNVM provides data privacy as the data is automatically corrupted between power cycles [156]. Therefore the adversary cannot retrieve the original data due to random errors. In order to see the effectiveness of this technique simulations are performed to observe the MTJ retention time. Fig. 22(a) shows the retention time with respect to the volume of the MTJ (varied by changing the free layer thickness). A 40-nm × 40-nm × 4-nm free layer is assumed for this simulations. As the size of the MTJ is lowered by 2X the retention time decreases from a few decades to a few seconds to realize SNVM. Fig. 22(b) shows the retention time dependence on temperature. Monte Carlo analysis was performed with 3σ of 5% for MTJ dimensions and with a mean retention time of 10 s. The cumulative distribution of the retention times under different temperatures (−50 °C to 100 °C) is shown in Fig. 22(b).

It is observed that the retention time can be very low at high temperature (min @100 °C = 9 ms), but increases dramatically by lowering the temperature (max @ − 50 °C ≈ 33 days). This can be exploited by the adversary to freeze the chip, increase the retention time and perform more exhaustive reverse engineering to access the data. Therefore, it is evident that SNVM could be a first line of defense but it cannot be used as a standalone technique to guarantee the privacy of LLC data.

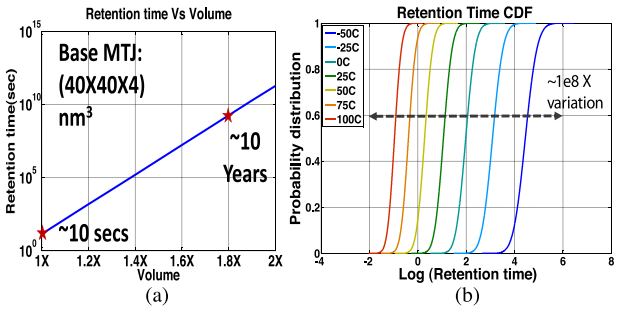

Fig. 22. ***(a) Retention time variation with respect to MTJ volume. (b) Retention time dependence on temperature [156].***

2) Data Erasure [156]: Access to LLC can be prevented by destroying (zeroizing in this case) the valid bit and tag. Erasing valid bit will ensure that an unauthorized read results in a miss. Similarly, erasing the tag will ensure that even if the valid is found set (due to random retention errors) the tag match will result in a mismatch (except when tag = 0) and the access is prevented. Finally, the data is also erased to ensure that even in the event of a hit due to random failures in valid/tag or tamper-assisted attack, the data obtained by the adversary is not authentic. Note that erasing at power ON will also destroy the data before being accessed by the adversary. However, the erasure at power OFF is preferable in order to prevent against power failure attack.

1) Clearing tag and data: The architecture [156] with features to erase the valid bit, tag, and data is shown in Fig. 23. It contains an extra multiplexer, decoder, counter, and register. The multiplexer (MUX1) is used to select the address coming from CPU (normal operation) or from the erase counter-I (erasing). When the system is turned OFF the erase signal ER is asserted (step 1) and a read signal is forced from the CPU. The erase counter has two parts namely, erase tag and erase index, the index is used to loop through the cache address space while the tag part erases the tag array (step 2). The zero index points to the first location and the corresponding tag may or may not match, in either of the situation the objective to erase is not hampered. Signal \ER is added as input to the AND gate that generates Hit/Miss. Since (\ER) is low it forces a read miss (step 3). A decoder with ER and Hit/Miss as input is used to bypass main memory and take the input from registers containing "0" data.

The data from the erase register is written in the data cache at index-0 and the tag which is all 0's is written in the tag array. Therefore the first location of the tag and data cache is erased successfully. Following this, the

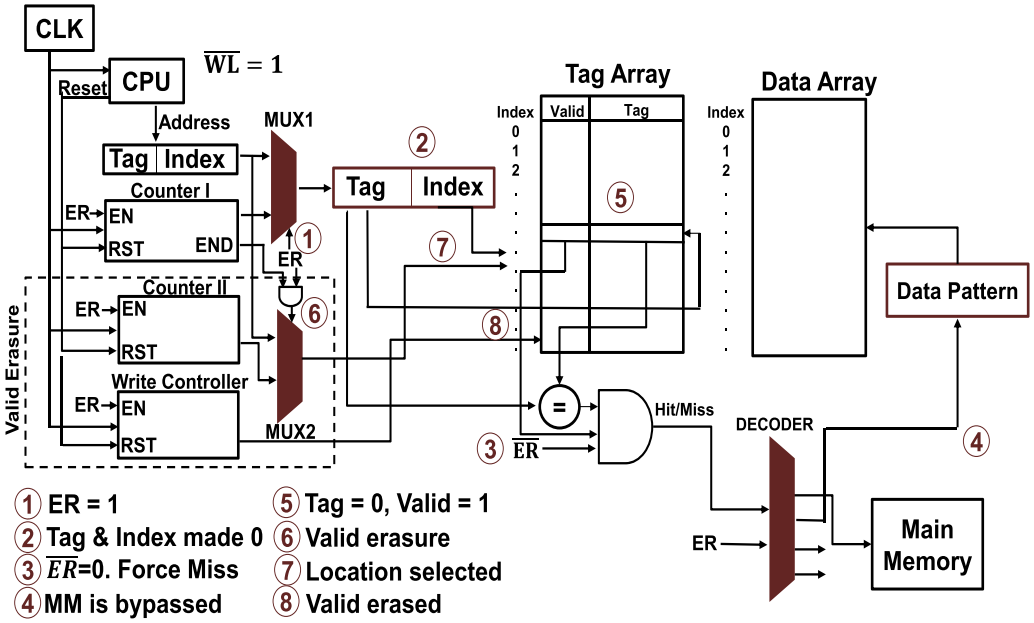

Fig. 23. ***The architecture to erase the cache tag, data and valid bits in a direct mapped cache when the system is turned off [156].***

erase counter is incremented and the next tag and data is erased. The same process is repeated to erase all tag and data bits. Note that although the tag and data bits are erased the valid bit is set for all locations after the erasing operation. During normal operation the ER signal is low and the main memory is selected instead of the erase register.

2) Clearing valid: The architecture to erase the valid bits is shown in the dotted rectangle in Fig. 5. A multiplexer (MUX2) is used to select the address from CPU (during normal operation) or the erase counter II (during erasing). The valid bits should be erased after the tag and data bits have been erased, as erasing tag and data will set the valid. Therefore, the multiplexer is controlled (step 6) by the END signal of the erase counter I. The erase counter II is initialized to zero (reset during system ON) thus points to the first address (step 7) in valid bit memory. The write controller writes "0" in the address location (step 8) and the counter II is incremented in the next cycle to erase the other locations. Apart from the above mentioned architecture every modern computer has a cache memory system with a controller which controls the clearing of valid bits according to the power ON signal or an instruction from the processor in case of change in virtual address space [170]. The same can be used by just adding one more signal at power OFF to erase the valid bits. Thus, in addition to power ON and an instruction from CPU, the controller must clear the valid bits at power OFF.

3) Erase Power Overhead and Mitigation [156]: Fig. 24(a) shows energy versus bit destruction. The erasure architecture [156] results is 0.6% IPC loss and 1.2% energy overhead during normal operation. From Fig. 24(a), we can observe that a reasonable amount of energy is required to perform 100% erasure. In normal shut down, this energy is easily available from the power supply, but, in case of power failure attacks, where the adversary intentionally removes the power supply to prevent erasure, an on-chip battery is needed. However, this is cost- and area-intensive. Another option is to perform erasure at power ON, which will achieve the same effect as erasure at power down; however, attacks such as probing during power down will go undetected.

VDD rail is a highly capacitive network which is fully charged even during power failure attack. It has been noted in [156] that this stored energy can be used to perform the erasure operation. Since erasure of each cache line consumes energy, the unregulated supply droops. To ensure erasure at lower voltages, it is important to prolong the write pulse width. Fig. 24(b) shows the MTJ write latency with the write voltage. A canary circuit is proposed in [156] to track the MTJ write time. The write pulse required to write the MTJ is generated with a Schmitt-trigger-based [171] MTJ canary circuit as shown in Fig. 8(a). The write pulse is dynamically tailored according to the instantaneous voltage by using a replica of the MTJ to generate the write pulse (Fig. 25). The idea is to write MTJ1 and MTJ2, sense the flipping using Schmitt triggers and generate a pulse that corresponds to MTJ write time. The pulse is used to drive the write driver performing erase. The transistors of the Schmitt trigger is biased to trigger when MTJs have flipped. The time taken for a MTJ to flip from AP to P state is less

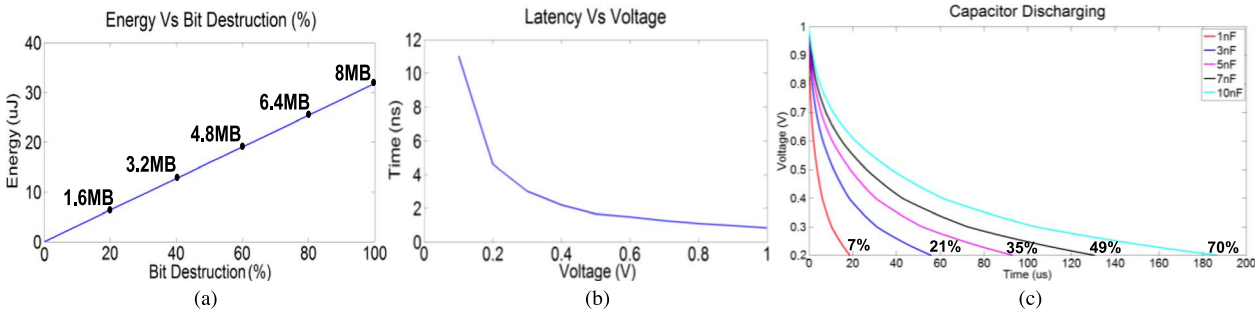

Fig. 24. *(a) Energy required to erase an 8 MB cache. (b) MTJ write latency variation with supply voltage. (c) Time taken to discharge and percentage erasure for an 8 MB cache with different capacitor value of power rail [156].*

than the time taken to flip from P to AP. The NAND gate is used to take this into account feed the J-K flip-flop that is used as a toggle flip flop. The write pulse is obtained from the Q' signal and is fed to the input (IN) node to create a ring oscillator.

Fig. 24(c) shows the discharge time and the erasure possible for different values of power rail capacitance. As the capacitance increases from 1 to 10 nF (typical for micro-processor), the number of bits that can be erased also increases. The energy of a 1-nF capacitor may not be sufficient to erase the whole cache, but it can easily erase the valid and tag bits which constitute 0.05% of an 8MB cache. Erasing tag and valid bits will make it difficult for the adversary to extract the user data from cache. The spice simulation shows that, if the power rails have 10 nF of capacitance, it can erase 70% of the cache without the need for any external power source like a battery. Note that supply rail energy can also be reused in other ways for massive erasure. Some techniques under consideration for future research are converting the energy into heat or magnetic field [156].

VII. FUTURE DIRECTIONS

A. Spintronic Hardware Security Primitives

The spintronic technology offers variety of security specific properties that can be tied with appropriate hardware security primitives. The recent literature has just started to explore some basic properties such as process variations in MTJ and magnetic nanowire for PUF design, stochastic MTJ dynamics for TRNG design and, serial access of DWM for encryption engines. However, a wide range of properties such as stochastic retention, statistical read/write performances, bifurcation of DW speed/phase and DW annihilation (as discussed in Section II) are still left unexplored. Design methodologies are required to extract the chaotic dynamics (such as bifurcation of DW speed or phase with respect to damping constant or

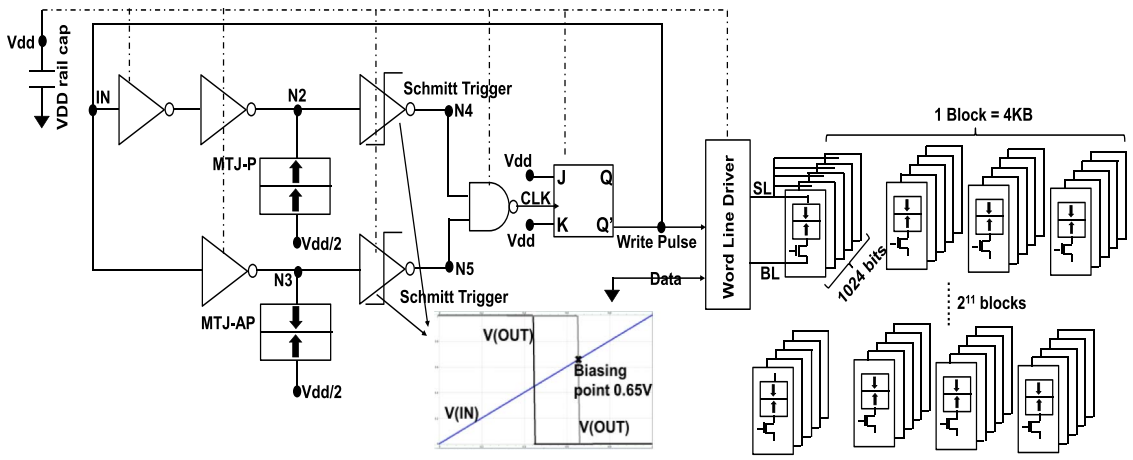

Fig. 25. *Schmitt trigger-based MTJ canary circuit [156].*

injected current density) and convert into measurable electrical quantities such as delay, current, voltage, and distance. Another fruitful direction is to explore the sensitivity of spintronic elements with respect to temperature, noise, and tampering to design novel hardware security primitives.

B. Data Security and Privacy

The awareness on data security issues associated with spintronic memory technologies (and NVMs in general) especially for cache applications has just started [155], [156]. Although magnetic tampering has been shown to be a possible mode of attack, other types of attacks are also possible. Furthermore, the purpose of attack could be more than destroying the content of cache. A careful adversary may launch other modes of attacks, namely side-channel attack, modulation of encryption keys, and so on. The new attack models need detailed investigation to assure the data security of NVM caches [193]–[195]. Since magnetic elements have shown promising results for logic computation and emerging application such as neuromorphic computation, research is pertinent to study the attack models and impact of various forms of tampering.

To ensure data privacy, new attack models and preventive techniques require further investigation. The attack models could differ to compromise data for each NVM cache hierarchy (ranging from L1 all the way to LLC). Research along the direction to avoid latency and power-intensive encryption can enable commercial deployment of NVMs in energy-constrained IoT. Extension of the attack models and preventive techniques to external memory would be an interesting research direction.

C. Prospects of Other Emerging Technologies

Besides spintronics, other emerging technologies such as memrister, PCM and ReRAM have also been explored from security perspective due to presence of noise and randomness such as one-time electroforming, random filament formation, and resistance variation [43]. Design of PUF using memristers [41]–[46], PCRAM [180] and ReRAM [181] have been proposed to exploit the process variation. ReRAM and memristers have also been shown to be promising technologies for TRNG [182], [183]. ReRAM technology is also employed to resist differential power attack (DPA) [140]. In PCRAM, limited write endurance is known as a potential weakness that can be exploited for tampering. Techniques such as randomized address mapping [141], DRAM buffer [142], and incremental encryption [143] is proposed to address this concern. In summary, other emerging technologies have also demonstrated significant potential to aid in securing the future systems. Therefore, hybrid systems with fusion of multiple emerging technologies can benefit significantly from the unique and complementary security features offered by these individual technologies.

VIII. SUMMARY

Apart from logic and memory applications, spintronic technology is appealing for hardware security due to the presence of noise, randomness, and chaos. As our understanding on these security properties are becoming more mature, there is a growing need to design hardware security primitives that exploit these properties. The recent research has been directed towards designing PUFs and TRNG by exploiting properties such as thermal noise and physical randomness using some specific spintronic devices such as STTRAM and DW nanowire. Nevertheless, there is wide gap between unexplored spintronic properties such as bifurcation of DW speed and phase, annihilation of DW, switching of DW type, nucleation of DW, susceptibility to temperature, magnetic field and laser, and, their applications in TRNG, recycling sensor, tamper detection sensor, and so on. The hardware security community will benefit immensely by understanding these properties and their security implications. With growing interest to adopt spintronic technology in future products, research on exploiting this technology for hardware security could be rewarding and impactful. We also highlighted the fundamental susceptibilities that could potentially become security vulnerabilities. New attacks could be launched using low-cost noninvasive techniques such as temperature or magnetic field with the intention to tamper the data. Along with security, the spintronic devices also bring privacy issues. The well-known encryption techniques will fail to prevent the security and privacy issues in emerging applications such as spintronic caches. Low-cost attack sensing and preventive solutions such as variable strength ECC and data erasure at power-down have shown encouraging results to mitigate data security and privacy attacks on spintronic cache. Further research directed towards exploring new policies and methodologies can benefit the commercialization of this promising technology. ■

Acknowledgment

The author would like to thank Dr. H. Naeimi, Prof. S. Bhunia, and Prof. J. Park for valuable discussions and the students at the LOGICS Lab, Pennsylvania State University and the University of South Florida.

REFERENCES

[1] M. Abramovici and P. Bradley, "Integrated circuit security—New threats and solutions," in *Proc. 5th Ann. Workshop Cyber Security Inf. Intell. Res.*, 2009, pp. 1–3.

[2] R. S. Chakraborty, S. Narasimhan, and S. Bhunia, "Hardware trojan: Threats and emerging solutions," *Proc. IEEE Int. High*

Level Design Validation Test Workshop, pp. 166–171, 2009.

[3] M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," *IEEE Design Test Comput.*, pp. 10–25, Jan.–Feb. 2010.

[4] S. Ali, D. Mukhopadhyay, R. S. Chakraborty, and S. Bhunia, "Multi-level attack: An emerging threat model for cryptographic hardware," *Proc. Design Autom. Test Eur.*, 2011.

[5] M. Rostami, F. Koushanfar, J. Rajendran, and R. Karri, "Hardware security: Threat models and metrics," in *Proc. Int. Conf. Comput.-Aided Design*, 2013, pp. 819–823.

[6] L. Lin, W. Burleson, and C. Paar, "MOLES: Malicious off-chip leakage enabled by side-channels," in *Proc. Int. Conf. Comput.-Aided Design*, 2009, pp. 117–122.

[7] M. Joye and J.-J. Quisquater, "Hessian elliptic curves and side-channel attacks," in *Cryptographic Hardware and Embedded Systems—CHES 2001*, pp. 402–410. Springer Berlin, Germany, 2001.

[8] *Gartner Says Worldwide Security Market to Grow 8.7 Percent in 2013*, Gartner, Inc., Jun. 11, 2013.

[9] J. Z. Sun *et al.*, "High-bias backhopping in nanosecond time-domain spin-torque switches of MgO-based magnetic tunnel junctions," *J. Appl. Phys.*, vol. 105, no. 7, 2009, Art. no. 07D109.

[10] SGMI Research Themes & Subjects. Online: http://www.samsung.com/global/business/semiconductor/html/news-events/file/SGMI_Request_for_Proposal.pdf

[11] H. Motaman, A. Iyengar, and S. Ghosh, "Synergistic circuit and system design for energy-efficient and robust Domain Wall caches," *Proc. IEEE Int. Symp. Low Power Electron. Design*, 2014.

[12] L. Zhang, X. Fong, C.-H. Chang, Z. H. Kong, and K. Roy, "Highly reliable memory-based physical unclonable function using spin-transfer torque MRAM," in *Proc. IEEE Int. Symp. Circuits Syst.*, 2014, pp. 2169–2172.

[13] J. Das, K. Scott, S. Rajaram, D. Burgett, and S. Bhanja, "MRAM PUF: A novel geometry based magnetic PUF with integrated CMOS," 2015.

[14] Y. Wang, H. Yu, D. Sylvester, and P. Kong, "Energy efficient in-memory AES encryption based on nonvolatile domain-wall nanowire," in *Proc. Design, Autom. Test in Europe Conf. Exhibition*, 2014, pp. 1–4.

[15] A. Fukushima *et al.*, "Spin dice: A scalable truly random number generator based on spintronics," *Appl. Phys. Exp.*, vol. 7, no. 8, 2014, Art. no. 083001.

[16] W. H. Choi *et al.*, "A magnetic tunnel junction based true random number generator with conditional perturb and real-time output probability tracking," in *Proc. IEEE Int. Electron Devices Meeting*, 2014, pp. 12–15.

[17] X. Fong, M.-C. Chen, and K. Roy, "Generating true random numbers using on-chip complementary polarizer spin-transfer torque magnetic tunnel junctions," in *Proc. 72nd Annu. Device Res. Conf.*, 2014, pp. 103–104.

[18] T. Weeks, Y. Lu, and X. Wang, "Magnetic precession based true random number generator," U.S. Patent Application 12/349,354, filed Jan. 6, 2009.

[19] X. Zhu, W. Wu, D. M. Jacobson, S. H. Kang, and K. H. Yuen, "Magnetic tunnel junction based random number generator," U.S. Patent Application 13/602,776, filed Sep. 4, 2012.

[20] K. Lee *et al.*, "Magnetic tunnel junction based random number generator," U.S. Patent Application 13/651,954, filed Oct. 15, 2012.

[21] W. Lin *et al.*, "Giant spin-dependent thermoelectric effect in magnetic tunnel junctions," *Nature Commun.*, vol. 3, 2012, p. 744.

[22] Z. Azim, X. Fong, T. Ostler, R. Chantrell, and K. Roy, "Laser induced magnetization reversal for detection in optical interconnects," 2014.

[23] D. Costello, and S. Lin, "Error control coding," New Jersey, 2004.

[24] J. Park, J. H. Choi, and K. Roy, "Dynamic bit-width adaptation in DCT: An approach to trade off image quality and computation energy," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 18, no. 5, May 2010, pp. 787–793.

[25] S. Paul, F. Cai, X. Zhang, and S. Bhunia, "Reliability-driven ECC allocation for multiple bit error resilience in processor cache," *IEEE Trans. Comput.*, vol. 60, no. 1, Jan. 2011, pp. 20–34.

[26] R. Pappu, "Physical one-way functions," Ph.D. dissertation, Mass. Inst. Technol., Cambridge, MA, USA, 2001.

[27] B. L. P. Gassend, "Physical random functions," Ph.D. dissertation, Mass. Inst. Technol., Cambridge, MA, USA, 2003.

[28] B. Gassend, D. Clarke, M. V. Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. 9th ACM Conf. Comput. Commun. Security*, 2002, pp. 148–160.

[29] B. Gassend, D. Lim, D. Clarke, M. V. Dijk, and S. Devadas, "Identification and authentication of integrated circuits," *Concurrency and Computation: Practice and Experience*, vol. 16, no. 11, 2004, pp. 1077–1098.

[30] P. Tuyls, G. Schrijen, B. Skoric, "Read-proof hardware from protective coatings," *CHES*, 2006, pp. 369–381.

[31] D. Lim *et al.*, "Extracting secret keys from integrated circuits," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 13, no. 10, Oct. 2005, pp. 1200–1205.

[32] G. E. Suh, S. Devadas, "Physical unclonable functions for device authentication and secret key generation," *Proc. DAC*, 2007, p. 914.

[33] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. V. Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *Symp. VLSI Circuits Dig. Tech. Papers*, pp. 176–179. IEEE, 2004.

[34] A. Maiti, J. Casarona, L. McHale, and P. Schaumont, "A large scale characterization of RO-PUF," in *Proc. IEEE Int. Symp. Hardware-Oriented Security and Trust*, 2010, pp. 94–99.

[35] Y. Su, J. Holleman, and B. Otis, "A 1.6J/bit 96% stable chip ID generating circuit using process variation," in *Proc. ISSCC*, 2007, pp. 406–611.

[36] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-up SRAM state as an identifying fingerprint and source of true random numbers," *IEEE Trans. Comput.*, vol. 58, no. 9, pp. 1198–1210, Sep. 2009.

[37] A. R. Krishna, S. Narasimhan, X. Wang, and S. Bhunia, "MECCA: A robust low-overhead PUF using embedded memory array," in *Proc. Cryptographic Hardware and Embedded Syst.*, 2011, pp. 407–420.

[38] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *Proc. Cryptographic Hardware and Embedded Syst.*, 2007, pp. 63–80.

[39] Y. Wang *et al.*, "Flash memory for ubiquitous hardware security functions: True random number generation and device fingerprints," in *Proc. IEEE Symp. Security and Privacy*, 2012, pp. 33–47.

[40] Y. Zheng, A. Krishna and S. Bhunia, "ScanPUF: Robust ultralow-overhead PUF using scan chain," *Proc. ASP-DAC*, 2013.

[41] G. S. Rose *et al.*, "Nanoelectronics and hardware security," *Netw. Sci. Cybersecurity*, pp. 105–123, 2014.

[42] G. S. Rose, N. McDonald, L.-K. Yan, B. Wysocki, and K. Xu, "Foundations of memristor based PUF architectures," in *Proc. IEEE/ACM Int. Symp. Nanoscale Architectures*, 2013, pp. 52–57.

[43] G. S. Rose *et al.*, "Hardware security strategies exploiting nanoelectronic circuits," in *Proc. ASP-DAC*, 2013, pp. 368–372.

[44] J. Rajendran, G. S. Rose, R. Karri, and M. Potkonjak, "Nano-PPUF: A memristor-based security primitive," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI*, 2012, pp. 84–87.

[45] J. Rajendran *et al.*, "Nanoelectronic solutions for hardware security," *IACR Cryptology ePrint Archive 2012*, 2012, p. 575.

[46] G. S. Rose, N. McDonald, L.-K. Yan, and B. Wysocki, "A write-time based memristive PUF for hardware security applications," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design*, 2013, pp. 830–833.

[47] X. Zhang and M. Tehranipoor, "Identification of recovered ICs using fingerprints from a light-weight on-chip sensor," in *Proc. Design Autom. Conf.*, 2012, pp. 703–708.

[48] X. Zhang and M. Tehranipoor, "Path-delay fingerprinting of identification of recovered ICs," in *Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst.*, Oct. 2012, pp. 13–18.

[49] X. Zhang and M. Tehranipoor, "Design of on-chip lightweight sensors for effective detection of recycled ICs," 2013, pp. 1–1.

[50] Nat. Inst. Standards Technol., Federal Information Processing Standard 197, The Advanced Encryption Standard (AES), 2001. [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[51] A. J. Elbwirt, W. Yip, B. Chetwynd, and C. Paar, "An FPGA implementation and performance evaluation of the AES block cipher candidate algorithm finalists," in *Proc. 3rd Advanced Encryption Standard Candidate Conf.*, 2000, pp. 13–27.

[52] K. Gaj and P. Chodowiec, "Comparison of the hardware performance of the AES candidates using reconfigurable hardware," in *Proc. 3rd Advanced Encryption Standard Candidate Conf.*, 2000, pp. 40–56.

[53] N. Weaver and J. Wawrzynek, "A comparison of the AES candidates amenability to FPGA implementation," in *Proc. 3rd Advanced Encryption Standard Candidate Conf.*, 2000, pp. 28–39.

[54] V. Fischer and M. Drutarovsky, "Two methods of rijndael implementation in reconfigurable hardware," in *Proc. Workshop*

Cryptographic Hardware and Embedded Syst., 2001, pp. 77–92.

[55] H. Kuo and I. Verbauwhede, "Architectural optimization for a 1.82 Gbits/Sec VLSI implementation of the AES rijndael algorithm," in *Proc. Workshop Cryptographic Hardware and Embedded Syst.*, 2001, pp. 51–64.

[56] M. McLoone and J. V. McCanny, "High performance single-chip FPGA Rijndael algorithm implementations," in *Proc. Workshop Cryptographic Hardware and Embedded Syst.*, 2001, pp. 65–76.

[57] A. Rudra *et al.*, "Efficient Rijndael encryption implementation with composite field arithmetic," in *Proc. Workshop Cryptographic Hardware and Embedded Syst.*, 2001, pp. 171–184.

[58] S. Mangard, M. Aigner, and S. Dominikus, "A highly regular and scalable AES hardware architecture," *IEEE Trans. Comput.*, vol. 52, no. 4, pp. 483–491, Apr. 2003.

[59] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, "A compact rijndael hardware architecture with S-box optimization," in *Proc. Advances in Cryptol.*, 2001, pp. 239–254.

[60] V. Rijmen, "Efficient Implementation of the Rijndael SBox," 2000. [Online]. Available: http://www.esat.kuleuven.ac.be/rijmen/rijndael/sbox.pdf

[61] J. Wolkerstorfer, E. Oswald, and M. Lamberger, "An ASIC implementation of the AES S-boxes," *Proc. RSA Conf. Topics in Cryptol.*, Feb. 2002.

[62] J. Wolkerstorfer, "An ASIC implementation of the AESMixColumn operation," *Proc. Austrochip*, Oct. 2001.

[63] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Advances in Cryptol.*, 1999, pp. 388–397.

[64] K. Tiri, M. Akmal, and I. Verbauwhede, "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards," *Proc. 28th Eur. Solid-State Circuits Conf.*, 2002.

[65] C. Petrie and J. Connelly, "A noise-based IC RNG for applications in cryptography," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 47, no. 5, pp. 615–621, May 2000.

[66] B. Jun and P. Kocher, "The Intel RNG," White Paper, 1999. [Online]. Available: http://www.cryptography.com/intelRNG.pdf

[67] V. Kaenel and T. Takayanagi, "Dual true random number generators for cryptographic applications embedded on a 200 million device dual CPU SOC," in *Proc. IEEE CICC*, 2007.

[68] J. Holleman, S. Bridges, B. Otis, and C. Diorio, "A 3 μW CMOS true random number generator with adaptive floating-gate offset cancellation," *IEEE J. Solid-State Circuits*, vol. 43, 5, pp. 1324–1336, May 2008.

[69] B. Sunar, W. Martin, and D. Stinson, "A provably secure TRNG with built-in tolerance to active attacks," *IEEE Trans. Comput.*, vol. 56, no. 1, pp. 109–119, Jan. 2007.

[70] R. Brederlow, R. Prakash, and C. Paulus, "A low-power TRNG using random telegraph noise of single oxide-traps," in *IEEE ISSCC Dig. Tech. Papers*, 2006, pp. 536–537.

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

[72] D. Schellekens, B. Preneel, and I. Verbauwhede, "FPGA vendor agnostic TRNG," in *Proc. 16th Int. IEEE Conf. Field Programmable Logic and Applications*, 2006, pp. 139–144.

[73] K. Wold and C. H. Tan, "Analysis and enhancement of random number generator in FPGA based on oscillator rings," in *Proc. Int. Conf. Reconfigurable Computing and FPGAs*, 2008, pp. 385–390.

[74] J. Golic, "New methods for digital generation, postprocessing of random data," *IEEE Trans. Comput.*, vol. 55, no. 10, pp. 1217–1229, Oct. 2006.

[75] M. Dichtl and J. Golic, "High-speed true random number generation with logic gates only," in *Proc. Cryptographic Hardware and Embedded Syst., LNCS 4727*, 2007, pp. 45–62.

[76] D. Kinniment and E. Chester, "Design of an on-chip random number generator using metastability," in *Proc. ESSCIRC*, 2002, pp. 595–598.

[77] C. Tokunaga, D. Blaauw, and T. Mudge, "True random number generator with a metastability-based quality control," *IEEE J. Solid-State Circuits*, vol. 43, no. 1, Jan. 2008, pp. 78–85.

[78] S. Srinivasan *et al.*, "2.4 GHz 7 mW all-digital PVT-variation tolerant TRNG in 45 nm CMOS," in *Symp. VLSI Circuits Dig. Tech. Papers*, 2010, pp. 216–217.

[79] S. Yasuda *et al.*, "Physical RNG based on MOS structure after soft breakdown," *IEEE J. Solid-State Circuits*, vol. 39, no. 8, pp. 1375–1377, Aug. 2004.

[80] N. Liu, N. Pinckney, S. Hansen, D. Sylvester, and D. Blaauw, "A TRNG using time-dependent dielectric breakdown," in *Symp. VLSI Circuits Dig. Tech. Papers*, 2011, pp. 216–217.

[81] M. Matsumoto *et al.*, "1200 m physical random-number generators based on Si-NMOSFET for secure smart-card application," in *IEEE ISSCC Dig. Tech. Papers*, 2008, pp. 414–415.

[82] S. Fujita *et al.*, "Si nanodevices for RNG circuits for cryptographic security," in *IEEE ISSCC Dig. Tech. Papers*, 2004, pp. 294–295.

[83] B. Jun and P. Kocher, "The intel random number generator," Cryptography Research Inc. white paper, 1999.

[84] S. A. Wolf *et al.*, "Spintronics: A spin-based electronics vision for the future," *Science*, vol. 294, no. 5546, 2001, pp. 1488–1495.

[85] I. Žutić, J. Fabian, and S. D. Sarma, "Spintronics: Fundamentals and applications," *Rev. Mod. Phys.*, vol. 76, no. 2, 2004, p. 323.

[86] S. Bandyopadhyay and M. Cahay, *Introduction to Spintronics*. Boca Raton, FL, USA: CRC, 2008.

[87] S. A. Wolf, J. Lu, M. R. Stan, E. Chen, and D. M. Treger, "The promise of nanomagnetics and spintronics for future logic and universal memory," in *Proc. IEEE*, vol. 98, no. 12, Dec. 2010, pp. 2155–2168.

[88] B. Behin-Aein, D. Datta, S. Salahuddin, and S. Datta, "Proposal for an all-spin logic device with built-in memory," *Nature Nanotechnol.*, vol. 5, no. 4, 2010, pp. 266–270.

[89] D. A. Allwood *et al.*, "Magnetic domain-wall logic," *Science*, vol. 309, no. 5741, 2005, pp. 1688–1692.

[90] G. Hrkac, J. Dean, and D. A. Allwood, "Nanowire spintronics for storage class memories and logic," *Phil. Trans. Royal Soc. A, Math. Phys., Eng. Sci.*, vol. 369, no. 1948, 2011, pp. 3214–3228.

[91] D. Morris, D. Bromberg, J.-G. J. Zhu, and L. Pileggi, "mLogic: Ultra-low voltage non-volatile logic circuits using STT-MTJ devices," in *Proc. 49th Annu. Design Autom. Conf.*, 2012, pp. 486–491.

[92] D. Nikonov and G. Bourianoff, "Taxonomy of Spintronics (a zoo of Devices)," 2006. [Online]. Available: http://nanohub.org/resources/1940

[93] K. Swaminathan, R. Pisolkar, C. Xu, and V. Narayanan, "When to forget: A system-level perspective on STT-RAMs," in *Proc. 17th Asia and South Pacific Design Autom. Conf.*, 2012, pp. 311–316.

[94] J. Li, P. Ndai, A. Goel, S. Salahuddin, and K. Roy, "Design paradigm for robust spin-torque transfer magnetic RAM (STT MRAM) from circuit/architecture perspective," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 18, no. 12, pp. 1710–1723, Dec. 2010.

[95] S. P. Park, S. Gupta, N. Mojumder, A. Raghunathan, and K. Roy, "Future cache design using STT MRAMs for improved energy efficiency: Devices, circuits and architecture," in *Proc. 49th Annu. Design Autom. Conf.*, 2012, pp. 492–497.

[96] A. Driskill-Smith, "Latest advances and future prospects of STT-RAM," in *Proc. Non-Volatile Memories Workshop*, 2010.

[97] Z. Diao, "Spin-transfer switching in MgO-based magnetic tunnel junctions," *J. Appl. Phys.*, vol. 99, no. 8, pp. 08G510–08G510, 2006.

[98] E. Y. Chen, Y. Huai, A. F. Panchula, L.-C. Wang, and X. Luo, "Current driven switching of magnetic storage cells utilizing spin transfer and magnetic memories using such cells having enhanced read and write margins," U.S. Patent 7 379 327, May 27, 2008.

[99] R. Beach *et al.*, "A statistical study of magnetic tunnel junctions for high-density spin torque transfer-MRAM (STT-MRAM)," in *Proc. IEEE Int. Electron Devices Meeting*, 2008, pp. 1–4.

[100] S. S. P. Parkin, M. Hayashi, and L. Thomas, "Magnetic domain-wall racetrack memory," *Science*, vol. 320, no. 5873, 2008, pp. 190–194.

[101] A. J. Annunziata *et al.*, "Racetrack memory cell array with integrated magnetic tunnel junction readout," in *Proc. IEEE Int. Electron Devices Meeting*, 2011, pp. 24–33.

[102] L. Thomas *et al.*, "Racetrack Memory: A high-performance, low-cost, non-volatile memory based on magnetic domain walls," in *Proc. IEEE Int. Electron Devices Meeting*, 2011, pp. 24–32.

[103] L. Thomas, M. Hayashi, X. Jiang, R. Moriya, C. Rettner, and S. S. P. Parkin,"Oscillatory dependence of current-driven magnetic domain wall motion on current pulse length," *Nature*, vol. 443, pp. 197–200, 2006.

[104] A. J. Annunziata *et al.*, "Racetrack memory cell array with integrated magnetic tunnel junction readout," in *Proc. IEEE Int. Electron Devices Meeting*, 2011, pp. 24–33. IEEE.

[105] M. Sharad, C. Augustine, G. Panagopoulos, and K. Roy, "Spin-based neuron model

with domain-wall magnets as synapse," *IEEE Trans. Nanotechnol.*, vol. 11, no. 4, Nov. 2012, pp. 843–853.

[106] M. Sharad, G. Panagopoulos, and K. Roy, "Spin neuron for ultra low power computational hardware," in *Proc. 70th Annu. Device Res. Conf.*, 2012, pp. 221–222.

[107] M. Sharad, C. Augustine, G. Panagopoulos, and K. Roy, "Proposal for Neuromorphic Hardware Using Spin Devices," arXiv preprint arXiv:1206.3227, 2012.

[108] M. Sharad, C. Augustine, G. Panagopoulos, and K. Roy, "Cognitive computing with spin-based neural networks," in *Proc. 49th Annu. Design Autom. Conf.*, 2012, pp. 1262–1263.

[109] M. Sharad, C. Augustine, and K. Roy, "Boolean and non-Boolean computation with spin devices," in *Proc. IEEE Int. Electron Devices Meeting*, 2012, pp. 11–16.

[110] M. Sharad, C. Augustine, G. Panagopoulos, and K. Roy, "Spin based neuron-synapse module for ultra low power programmable computational networks," in *Proc. Int. Joint Conf. Neural Netw.*, 2012, pp. 1–7.

[111] L. Berger, "Exchange interaction between ferromagnetic domain-wall and electric-current in very thin metallic-films," *J. Appl. Phys.*, vol. 55, pp. 1954–1956, 1984.

[112] L. Berger, "Motion of a magnetic domain-wall traversed by fast-rising current pulses," *J. Appl. Phys.*, vol. 71, pp. 2721–2726, 1992.

[113] P. P. Freitas and L. Berger, "Observation of s-d exchange force between domain-walls and electric-current in very thin permalloy-films," *J. Appl. Phys.*, vol. 57, pp. 1266–1269, 1985.

[114] C. Y. Hung and L. Berger, "Exchange forces between domain-wall and electric-current in permalloy-films of variable thickness," *J. Appl. Phys.*, vol. 63, pp. 4276–4278, 1988. Part 3.

[115] C. Y. Hung, L. Berger, and C. Y. Shih, "Observation of a current-induced force on Bloch lines in Ni-Fe thin-films," *J. Appl. Phys.*, vol. 67, pp. 5941–5943, 1990. Part 2B.

[116] E. Salhi and L. Berger, "Current-induced displacements and precession of a Bloch wall in Ni-Fe thin-films," *J. Appl. Phys.*, vol. 73, pp. 6405–6407, 1993. Part 2B.

[117] E. Salhi and L. Berger, "Current-induced displacements of Bloch walls in Ni-Fe films of thickness 120–740 nm," *J. Appl. Phys.*, vol. 76, pp. 4787–4792, 1994.

[118] M. Hayashi, "Current driven dynamics of magnetic domain walls in permalloy nanowires," Ph.D. dissertation, Stanford Univ., Stanford, CA, USA, 2006.

[119] S. X. Wang, and A. M. Taratorin, *Magnetic Information Storage Technology: A Volume in the Electromagnetism Series*. Academic, New York, NY, USA, 1999.

[120] J. Zhang, P. M. Levy, S. Zhang, and V. Antropov, "Identification of transverse spin currents in noncollinear magnetic structures," *Phys. Rev. Lett.*, vol. 93, no. 25, 2004, Art. no. 256602.

[121] A. Thiaville and Y. Nakatani, "Domain-wall dynamics in nanowires and nanostrips," in *Spin Dynamics in Confined Magnetic Structures III*, pp. 161–205. Springer Berlin, Germany, 2006.

[122] D. FitzPatrick and I. Miller, *Analog Behavioral Modeling With the Verilog-A Language*. Springer, Berlin, Germany, 1998.

[123] R. A. Duine, A. S. Núñez, and A. H. MacDonald, "Thermally assisted current-driven domain-wall motion," *Phys. Rev. Lett.*, vol. 98, no. 5, 2007, Art. no. 056605.

[124] G. Meier *et al.*, "Direct imaging of stochastic domain-wall motion driven by nanosecond current pulses," *Phys. Rev. Lett.*, vol. 98, no. 18, 2007, Art. no. 187202.

[125] L. Thomas, R. Moriya, C. Rettner, and S. SP Parkin, "Dynamics of magnetic domain walls under their own inertia," *Science*, vol. 330, no. 6012, 2010, pp. 1810–1813.

[126] D. G. Hermann and J.-P. Nguenang, "Chaos Appearance during domain wall motion under electronic transfer in nanomagnets," *World J. Condensed Matter Phys.*, vol. 3, 2013, p. 136.

[127] H. Okuno, "Chaos and energy loss of nonlinear domain wall motion," *J. Appl. Phys.*, vol. 81, no. 8, 1997, pp. 5233–5235.

[128] R. Hertel, W. Wulfhekel, and J. Kirschner, "Domain-wall induced phase shifts in spin waves," *Phys. Rev. Lett.*, vol. 93, no. 25, 2004, Art. no. 257202.

[129] Z. Li, J. He, and S. Zhang, "Magnetization instability driven by spin torques," *J. Appl. Phys.*, vol. 97, no. 10, 2005, Art. no. 10C703.

[130] K. N. Alekseev, G. P. Berman, V. I. Tsifrinovich, and A. M. Frishman, "Dynamical chaos in magnetic systems," *Soviet Phys. Uspekhi*, vol. 35, no. 7, 1992, p. 572.

[131] F.-X. Hu, B.-G. Shen, and J.-R. Sun, "Magnetic entropy change in Ni 51.5 Mn 22.7 Ga 25.8 alloy," *Appl. Phys. Lett.*, vol. 76, no. 23, 2000, pp. 3460–3462.

[132] E. Ott, *Chaos in Dynamical Systems*. Cambridge Univ., Cambridge, U.K., 2002.

[133] M. Jamali, K.-J. Lee, and H. Yang, "Metastable magnetic domain wall dynamics," *New J. Phys.*, vol. 14, no. 3, 2012, Art. no. 033010.

[134] C. Burrowes *et al.*, "Role of pinning in current driven domain wall motion in wires with perpendicular anisotropy," *Appl. Phys. Lett.*, vol. 93, no. 17, 2008, Art. no. 172513.

[135] A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications, National Inst. Standards and Technol., Pub 800-22, 2010.

[136] L. Chua, "Memristor—The missing circuit element," *IEEE Trans. Circuit Theory*, vol. CT-18, no. 5, 1971, pp. 507–519.

[137] D. B. Strukov, G. S. Snider, D. R. Stewart, and R. S. Williams, "The missing memristor found," *Nature*, vol. 453, no. 7191, 2008, pp. 80–83.

[138] R. Williams, "How we found the missing memristor," *IEEE Spectrum*, vol. 45, no. 12, 2008, pp. 28–35.

[139] Y. N. Joglekar and S. J. Wolf, "The elusive memristor: Properties of basic electrical circuits," *Eur. J. Phys.*, vol. 30, no. 4, 2009, p. 661.

[140] G. Khedkar and D. Kudithipudi, "RRAM motifs for mitigating differential power analysis attacks (DPA)," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI*, 2012, pp. 88–93.

[141] M. K. Qureshi *et al.*, "Enhancing lifetime and security of PCM-based main memory with start-gap wear leveling," in *Proc. 42nd Annu. IEEE/ACM Int. Symp. Microarchitecture*, 2009, pp. 14–23.

[142] N. H. Seong, D. H. Woo, and H.-H. S. Lee, "Security refresh: Prevent malicious wear-out and increase durability for phase-change memory with dynamically randomized address mapping," in *ACM SIGARCH Computer Architecture News*, vol. 38, no. 3, 2010, pp. 383–394.

[143] S. Chhabra and D. Solihin, "i-NVMM: A secure non-volatile main memory system with incremental encryption," in *Proc. 38th Annu. Int. Symp. Computer Architecture*, 2011, pp. 177–188.

[144] B. D. Long, Y. B. Li, and R. Jha, "Switching characteristics of Ru/HfO2/TiO2-x/Ru RRAM devices for digital and analog nonvolatile memory applications," *IEEE Electron. Device Lett.*, 2012, vol. 33, pp. 706–708, doi: 10.1109/led.2012.2188775.

[145] B. D. Long, Y. B. Li, S. Mandal, R. Jha, and K. Leedy, "Switching dynamics and charge transport studies of resistive random access memory devices," *Appl. Phys. Lett.*, 2012, vol. 101, doi: 10.1063/1.4749809.

[146] B. M. Long, S. Mandal, J. Livecchi, and R. Jha, "Effects of Mg-doping on HfO2-based ReRAM device switching characteristics," *IEEE Electron Device Lett.*, 2013, vol 34, pp. 1247–1249, doi:10.1109/led.2013.2276482.

[147] S. Mandal, B. Long, and R. Jha, "Study of synaptic behavior in doped transition metal oxide-based reconfigurable devices," *IEEE Trans. Electron Devices*, 2013, vol. 60, pp. 4219–4225, doi:10.1109/ted.2013.2288327.

[148] M. J. Donahue, and D. G. Porter, *OOMMF User's Guide*. U.S. Dept. of Commerce, Technol. Administration, Nat. Inst. of Standards and Technol., 1999.

[149] J. Rajendran *et al.*, "Nano meets security: Exploring nanoelectronic devices for security applications," 2015.

[150] S. Skorobogatov, *Low Temperature Data Remanence in Static RAM*. Univ. Cambridge Comput. Lab., 2001.

[151] K. Swaminathan, R. Pisolkar, C. Xu, and V. Narayanan, "When to forget: A system-level perspective on STT-RAMs," in *Proc. 17th Asia and South Pacific Design Autom. Conf.*, 2012, pp. 311–316.

[152] J. A. Halderman, "Lest we remember: Cold-boot attacks on encryption keys," *Commun. ACM*, vol. 52, no. 5, 2009, pp. 91–98.

[153] A. Iyengar, S. Ghosh, and K. Ramclam, "Domain wall magnet for embedded memory and hardware security," *J. Emerging Topics on Circuits Syst.*, 2015.

[154] A. Iyengar, K. Ramclam, and S. Ghosh, "DWM-PUF: A low-overhead, memory-based security primitive," in *Proc. IEEE Int. Symp. Hardware-Oriented Security and Trust*, 2014, pp. 154–159. IEEE.

[155] A. Iyengar, S. Ghosh, K. Ramclam, J.-W. Jang, and C.-W. Lin, "Spintronic PUFs for security, trust and authentication," *JETC*, 2015.

[156] N. Rathi, S. Ghosh, A. Iyengar, and H. Naeimi, "Data privacy in non-volatile cache: Challenges, attack models and solutions," *Proc. ASPDAC*, 2016.

[157] Domain Wall Memory: The Next Big Thing in Hardware Security? IEEE Xplore INNOVATION SPOTLIGHT, 2015.

[158] J.-W. Jang, J. Park, S. Ghosh, and S. Bhunia, "Self-correcting STTRAM under

magnetic field attacks," in *Proc. 52nd Annu. Design Autom. Conf.*, 2015, p. 77.

[159] A. Iyengar and S. Ghosh, "Modeling and analysis of domain wall dynamics for robust and low-power embedded memory," *Proc. IEEE Design Autom. Conf.*, 2014.

[160] S. Ghosh and R. Govindraj, "Spintronics for associative computation and hardware security," *Proc. MWSCAS*, 2015.

[161] [Online]. Available: http://en.wikipedia.org/wiki/Magnet

[162] J. Daemen and V. Rijmen, *The Design of Rijndael: AES-The Advanced Encryption Standard*. Springer, Berlin, Germany, 2002.

[163] A. Maiti, V. Gunreddy, and P. Schaumont, "A systematic method to evaluate and compare the performance of physical unclonable functions," in *Embedded Systems Design with FPGAs*, pp. 245–267. Springer New York, NY, USA, 2013.

[164] W. Burleson, Hardware Security in Nanometer CMOS. [Online]. Available: http://sti.epfl.ch/files/content/sites/sti/files/shared/sel/pdf/Talk_Burleson_EE-SRI_2011.pdf

[165] S. Ghosh, "Design methodologies for high density domain wall memory," in *Proc. IEEE Int. Symp. Nanoscaled Architecture*, 2013.

[166] S. Ghosh, "Path to a teraByte of on-chip memory for petabit per second bandwidth with < 5 Watts of power," in *Proc. 50th Annu. Design Autom. Conf.*, 2013, p. 145.

[167] N. D. Rizzo *et al.*, "A fully functional 64 Mb DDR3 ST-MRAM built on 90 nm CMOS technology," *IEEE Trans. Magn.*, vol. 49, no. 7, pp. 4441–4446, Jul. 2013.

[168] M. H. Kryder and C. S. Kim, "After hard drives—What comes next?" *IEEE Trans. Magn.*, vol. 45, no. 10, 2009, pp. 3406–3413.

[169] S. H. Weingart, "Physical security devices for computer subsystems: A survey of attacks and defenses," *Proc. Cryptographic Hardware and Embedded Syst.*, 2000.

[170] Y. Kobayashi and T. Rokutanda, "Cache memory control system," U.S. Patent 4 219 883, issued Aug. 26, 1980.

[171] M. R. Jan, C. Anantha, and N. Borivoje, "Digital Integrated Circuits-A Design Perspective," 2002.

[172] Predictive Technology Model, ASU. [Online]. Available: http://www.asu.edu/; ptm

[173] T. Tanamoto *et al.*, "High-speed magnetoresistive random-access memory random number generator using error-correcting code," *Jpn. J. Appl. Phys.*, vol. 50, no. 4, 2011, Art. no. 04DM01.

[174] Y. Oishi *et al.*, "Random number generating device, random number generating method, and security chip," U.S. Patent 8 351 ,603, issued Jan. 8, 2013.

[175] A. Nigam *et al.*, "Delivering on the promise of universal memory for spin-transfer torque RAM (STT-RAM)," in *Proc. 17th IEEE/ACM Int. Symp. Low-Power Electron. Design*, 2011, pp. 121–126.

[176] P. Weiss, "L'hypothèse du champ moléculaire et la propriété ferromagnétique," *J. Phys. Theor. Appl.*, vol. 6, no. 1, 1907, pp. 661–690.

[177] A. Raghunathan *et al.*, "Modeling the temperature dependence of hysteresis based on Jiles-Atherton theory," *IEEE Trans. Magn.*, vol. 45, no. 10, Oct. 2009, pp. 3954–3957.

[178] C. H. Shang, J. Nowak, R. Jansen, and J. S. Moodera, "Temperature dependence of magnetoresistance and surface magnetization in ferromagnetic tunnel junctions," *Phys. Rev. B*, vol. 58, no. 6, 1998, Art. no. R2917.

[179] Y. Lu *et al.*, "Bias voltage and temperature dependence of magnetotunneling effect," *J. Appl. Phys.*, vol. 83, no. 11, 1998, pp. 6515–6517.

[180] L. Zhang, Z. H. Kong, C.-H. Chang, A. Cabrini, and G. Torelli, "Exploiting process variations and programming sensitivity of phase change memory for reconfigurable physical unclonable functions," *IEEE Trans. Inf. Forensics and Security*, vol. 9, no. 6, 2014, pp. 921–932.

[181] P.-Y. Chen, "Exploiting resistive cross-point array for compact design of physical unclonable function," in *Proc. Int. Symp. Hardware Oriented Security and Trust*, pp. 26–31, 2015.

[182] Y. T. Chiu, "A Memristor true random-number generator," *IEEE Spectrum*, 2012.

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

[184] H. Naeimi, C. Augustine, A. Raychowdhury, S.-L. Lu, and J. Tschanz, "STTRAM scaling and retention failure," *Intel Technol. J.*, vol. 17, no. 1, 2013, pp. 54–75.

[185] R. Bishnoi, M. Ebrahimi, F. Oboril, and M. B. Tahoori, "Read disturb fault detection in STT-MRAM," in *Proc. IEEE Int. Test Conf.*, 2014, pp. 1–7.

[186] Y. Ran, W. Kang, Y. Zhang, J.-O. Klein, and W. Zhao, "Read disturbance issue for nanoscale STT-MRAM," in *Proc. IEEE Non-Volatile Memory System and Applications Symp.*, 2015, pp. 1–6.

[187] M. Nakayama *et al.*, "Spin transfer switching in TbCoFe/CoFeB/MgO/CoFeB/TbCoFe magnetic tunnel junctions with perpendicular magnetic anisotropy," *J. Appl. Phys.*, vol. 103, no. 7, 2008, pp. 07A710–07A710.

[188] A. Panchula, "Oscillating-field assisted spin torque switching of a magnetic tunnel junction memory element," U.S. Patent 7 224 601, issued May 29, 2007.

[189] A. A. Tulapurkar *et al.*, "Spin-torque diode effect in magnetic tunnel junctions," *Nature*, vol. 438, no. 7066, 2005, pp. 339–342.

[190] C. Werndl, "What are the new implications of chaos for unpredictability?" *Brit. J. Phil. Sci.*, vol. 60, no. 1, 2009, pp. 195–220.

[191] Y. Suzuki, A. A. Tulapurkar, and C. Chapp, *Nanomagnetism and Spintronics*, 1st ed. Elsevier, Amsterdam, The Netherlands, 2008, ch. 3.

[192] J.-W. Jang and S. Ghosh, "Performance impact of magnetic and thermal attacks on STTRAM and low-overhead mitigation techniques," *Proc. IEEE Int. Symp. Low Power Electron. Design*, 2016.

[193] N. Rathi, A. De, H. Naeimi, and S. Ghosh, "Cache bypassing and checkpointing to circumvent data security attacks on STTRAM," arXiv preprint arXiv:1603.06227 (2016).

[194] N. Rathi, H. Naeimi, and S. Ghosh, "Side channel attacks on STTRAM and low-overhead countermeasures," arXiv preprint arXiv:1603.06675 (2016).

[195] A. De, M. N. I. Khan, and S. Ghosh, "Attack resilient architecture to replace embedded flash with STTRAM in homogeneous IoTs," arXiv preprint arXiv:1606.00467 (2016).

ABOUT THE AUTHOR

Swaroop Ghosh (Senior Member, IEEE) received the B.E. (honors) degree from the Indian Institute of Technology, Roorkee, India, in 2000, the M.S. degree from the University of Cincinnati, Cincinnati, OH, USA, in 2004, and the Ph.D. degree from Purdue University, West Lafayette, IN, USA, 2008.

He joined Pennsylvania State University, University Park, PA, USA, in fall 2016. From 2012 to 2016, he was a Member of Faculty with USF. He was a Senior Research and Development Engineer with Advanced Design, Intel Corporation, from 2008 to 2012. His research interests include low-power circuit design and hardware security.

Dr. Ghosh has served as an Associate Editor of the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS I: REGULAR PAPERS and a Senior Editorial board Member of the IEEE JOURNAL ON EMERGING AND SELECTED TOPICS IN CIRCUITS AND SYSTEMS. He has served on the technical program committees of DAC, DATE, ICCAD, CICC, ISLPED, HOST, Nanoarch, VLSI Design, ISQED, ASQED, and VLSI-SOC. He was a recipient of the DARPA Young Faculty Award in 2015, the ACM SIGDA Outstanding New Faculty Award in 2016, the USF Outstanding Research Achievement Award in 2015, and the USF College of Engineering Outstanding Research Achievement Award in 2015.