IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 3, 2020, accepted April 16, 2020, date of publication April 20, 2020, date of current version May 6, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2988889

SMART: A Secure Magnetoelectric AntifeRromagnet-Based Tamper-Proof Non-Volatile Memory

NIKHIL RANGARAJAN[1], (Member, IEEE), SATWIK PATNAIK[2], (Graduate Student Member, IEEE), JOHANN KNECHTEL[1], (Member, IEEE), OZGUR SINANOGLU[1], (Senior Member, IEEE), AND SHALOO RAKHEJA[3], (Member, IEEE)

[1]Division of Engineering, New York University Abu Dhabi (NYU AD), Abu Dhabi 129188, United Arab Emirates
[2]Department of Electrical and Computer Engineering, New York University (NYU), Brooklyn, NY 11201, USA
[3]Holonyak Micro and Nanotechnology Laboratory, University of Illinois at Urbana–Champaign (UIUC), Urbana, IL 61801, USA

Corresponding authors: Nikhil Rangarajan (nikhil.rangarajan@nyu.edu), Satwik Patnaik (sp4012@nyu.edu), and Shaloo Rakheja (rakheja@illinois.edu)

This work was supported in part by the Semiconductor Research Corporation (SRC) and the National Science Foundation (NSF) through the grant ECCS 1740136. The work of Satwik Patnaik was supported by the Global Ph.D. Fellowship at NYU/NYU AD.

ABSTRACT The storage industry is moving toward emerging non-volatile memories (NVMs), including the spin-transfer torque magnetoresistive random-access memory (STT-MRAM) and the phase-change memory (PCM), owing to their high density and low-power operation. In this paper, we demonstrate, for the first time, circuit models and performance benchmarking for the domain wall (DW) reversal-based magnetoelectric-antiferromagnetic random access memory (ME-AFMRAM) at cell-level and at array-level. We also provide perspectives for coherent rotation-based memory switching with topological insulator-driven anomalous Hall read-out. In the coherent rotation regime, the ultra-low power magnetoelectric switching coupled with the terahertz-range antiferromagnetic dynamics result in substantially lower energy-per-bit and latency metrics for the ME-AFMRAM compared to other NVMs including STT-MRAM and PCM. After characterizing the novel ME-AFMRAM, we leverage its unique properties to build a dense, on-chip, secure NVM platform, called *SMART: A Secure Magnetoelectric Antiferromagnet-Based Tamper-Proof Non-Volatile Memory*. New NVM technologies open up challenges and opportunities from a data-security perspective. For example, their sensitivity to magnetic fields and temperature fluctuations, and their data remanence after power-down make NVMs vulnerable to data theft and tampering attacks. The proposed SMART memory is not only resilient against data confidentiality attacks seeking to leak sensitive information but also ensures data integrity and prevents Denial-of-Service (DoS) attacks on the memory. It is impervious to particular power side-channel (PSC) attacks that exploit asymmetric read/write signatures for '0' and '1' logic levels, and photonic side-channel attacks that monitor photo-emission signatures from the chip backside.

INDEX TERMS Antiferromagnetic materials, magnetoelectric effects, non-volatile memory, tamper-proof memory, magnetic memory.

I. INTRODUCTION AND BACKGROUND

Conventional dynamic random-access memory (DRAM) scaling has reached a critical tipping point as the miniaturization of the DRAM cell has plateaued in recent years. Feature size scaling below the 20 nm technology node is met with numerous challenges such as shorter retention times, higher leakage currents, and increased fault rates [1]. Solutions to address these concerns include improved DRAM fault detection and recovery [2], as well as architectural techniques to enhance DRAM scaling [3].

A promising solution to the memory scaling problem is to realize the main memory system using non-volatile technologies [4]. Examples of emerging non-volatile

The associate editor coordinating the review of this manuscript and approving it for publication was Guijun Li.

memories (NVMs) include spin-transfer torque magnetoresistive random-access memory (STT-MRAM), ferroelectric random-access memory (FeRAM), resistive random-access memory (ReRAM), and phase-change memory (PCM). Interest in the commercial application of such NVMs has increased significantly. For instance, Intel's current line of 3D XPoint memory systems utilize PCM-based NVM technology [5], and IBM and Everspin's solid-state drive comes with STT-MRAM write caches [6]. While NVMs offer attractive features, such as high density, low leakage, and non-volatile data retention, they also suffer from poor endurance and high access latency in their current implementation.

Memory security has come under more scrutiny over the years. This is because of attacks such as *Spectre* [7] and *Meltdown* [8], which targets the side-channels associated with speculative execution and out-of-order execution, respectively, have exposed severe vulnerabilities in a wide array of currently deployed processors and their memory architectures. In the case of NVMs, data remanence after power-down presents a severe threat to data confidentiality, as attackers aiming to steal private data can do so easily by mounting cold-boot attacks [9] or other removal attacks like stealing the memory module (DIMM) [10]. Moreover, magnetic memories like STT-MRAM are highly sensitive to stray magnetic fields. As such, magnetic field-based attacks [11] can be used to corrupt the stored data or compromise the memory's functional integrity, resulting in a denial-of-service (DoS) attack. Hence, such security vulnerabilities pose a significant impediment to the pervasive and large-scale proliferation of NVMs in the memory industry.

A. RELATED WORK IN MEMORY SECURITY

Prior works on securing NVMs have focused mainly on memory encryption schemes, which are necessary to prevent attackers from exploiting data remanence in the off-state. Chhabra *et al.* proposed an incremental encryption scheme [12] for NVMs where only inert memory pages, which have not been accessed for several clock cycles, are encrypted selectively. The working set of the memory (which is in current use) is in plaintext and, hence, incurs no encryption overhead on access. Such a selective encryption ensures that the majority of the main memory content (but not all) remains encrypted at all times, without overly compromising the performance. However, it requires dedicated hardware, inert page prediction, and scheduling for its implementation. A sneak-path encryption (SPE) scheme was demonstrated for memristor-based NVMs in [13], wherein sneak paths in the memristor crossbar array are exploited to apply encryption pulses to change the resistances of the memory cells, and hence, encrypt the stored data.

In [10], the authors proposed DEUCE, a dual counter encryption for PCM memories, which significantly reduces the number of modified bits per writeback, to improve performance and lifetime of the memory. This scheme aims to mitigate the impact of the avalanche effect [14] occurring during memory encryption, by re-encrypting and writing back only the modified words during any write operation. Swami *et al.* took this concept forward and proposed SECRET [15], a smart encryption scheme for NVMs, which integrates word-level re-encryption and zero-based partial writes to reduce memory write operations. They also demonstrate write optimization through the use of ''energy masks'' (i.e., bit templates XORed with ciphertext to obtain lower energy dissipation) in the encryption XOR logic, which minimizes the bit flips in the encryption process, thereby reducing the total write energy. An advanced counter-mode encryption (ACME) was presented in [16], which utilizes the write leveling architecture inherent in PCM memories, to perform counter-write leveling. ACME helps to avoid *Rowhammer*-type attacks by preventing the counter associated with any single cache line from overflowing.

The impact of contactless tampering on STT-MRAMs using external magnetic fields was highlighted in [11]. Using micromagnetic simulations, the authors of [11] showed how magnetic field-based attacks could corrupt the contents of STT-MRAM cells. Techniques to protect against contactless attacks proposed in [11] included (i) an on-chip sensor to detect magnetic field-based incursions, and (ii) error correction modules to compensate cell failures arising due to magnetic field attacks. However, these techniques incur large energy and area penalties due to the additional hardware imposed by the magnetic field sensor and the error correction scheme.

B. CONTRIBUTIONS

In this paper, we present an alternative to conventional NVMs such as STT-MRAM and PCM, in the form of *SMART: A Secure Magnetoelectric Antiferromagnet-Based Tamper-Proof Non-Volatile Memory*. SMART memory leverages the room-temperature linear magnetoelectric (ME) effect in antiferromagnets (AFMs) like chromia [17], which can be switched solely using voltage pulses, without the use of electric currents, leading to ultra-low energy ($\sim$ pico-Joules) operation. Further, the intrinsic dynamics of AFMs is typically in the terahertz regime ($\sim$ 10^{12} Hz) [18], which could enable picosecond time-scale reversal of the AFM domain. In addition to its energy and latency benefits, SMART memory offers a significant advancement in terms of secure and tamper-proof data storage. For example, AFMs do not exhibit a magnetic signature since they do not have a net external magnetic moment, unlike ferromagnets (FM). Hence, the SMART memory cannot be probed or switched with external magnetic fields, unlike the way STT-MRAMs can. This, in turn, eliminates the possibility of magnetic field attacks undermining data integrity or aiming to induce DoS. To address the post-shutdown data remanence of SMART memory, we demonstrate an in-memory encryption scheme employing ME-AFM transistor-based controlled-NOT (CNOT) logic. We discuss the resilience of the SMART memory against attacks aiming to undermine data confidentiality and data fidelity, in both powered-on and powered-off

states. The main contributions of this work can be summarized as follows:

1) We discuss the design of SMART, a secure ME-AFM-based NVM and implement its SPICE circuit model to simulate the memory performance.
2) We demonstrate the resilience of SMART memory against magnetic field and temperature attacks, which can affect other NVMs like STT-MRAM. We explore the implications of various side-channel attacks on the SMART memory.
3) We present an in-memory encryption scheme with ME-AFM transistor-based CNOT gates, called *Memcryption*, to protect the data stored in SMART memory against cold-boot and stolen DIMM attacks, while incurring low encryption latency overheads. We like to mention here that *Memcryption* is specifically tailored for the ME-AFMRAM, not for a generic NVM. Also, it does not secure the memory system against *bus snooping* attacks; such attacks are beyond the scope of this work.

In the next section, we describe the modeling, implementation and benchmarking of the proposed ME-AFM memory both at cell- and array-level, before proceeding to evaluate its security properties in Section III.

II. DEVICE MODEL AND FUNCTIONALITY

A. THE MAGNETOELECTRIC EFFECT

The linear ME effect [19] represents the coupling between applied magnetic field and induced polarization or between applied electric field and induced magnetization in non-centrosymmetric crystals like chromia (Cr_2O_3). Compared to the STT-based magnetization reversal of FMs requiring electric currents on the order of $\sim 10^6$ A/cm^2 and incurring associated Joule heating, the ME effect provides an energy-efficient, all-electrical switching of the roughness-insensitive boundary magnetization of chromia [20]. Additionally, chromia is an AFM; hence, the net bulk magnetic moment (i.e., the difference of the sublattice magnetization vectors) vanishes and becomes imperceptible externally. However, the boundary magnetization is strongly coupled to the AFM order parameter. That is, the electrical switching of the AFM order results in reversal of the boundary magnetization [21], which is used to encode the information in ME-AFM memories.

The uncompensated surface moments at the (0001) surface of chromia result in an equilibrium boundary magnetization, which could be in one of the two oppositely aligned, degenerate domain states. The degeneracy between the domains is lifted through ME annealing, which allows the preferential selection of one of the states [22]. That is, the ME annealing polarizes the surface and results in a single-domain surface moment. Isothermal switching between these single domain states using an electric field E and a small, symmetry-breaking DC magnetic field H has been demonstrated experimentally [22], [23]. The critical condition for such ME switching is that the magnitude of the $E \cdot H$ product must exceed the ME threshold energy barrier, which was shown experimentally to be as low as ≈ 1 J/m^3 [24], [25].

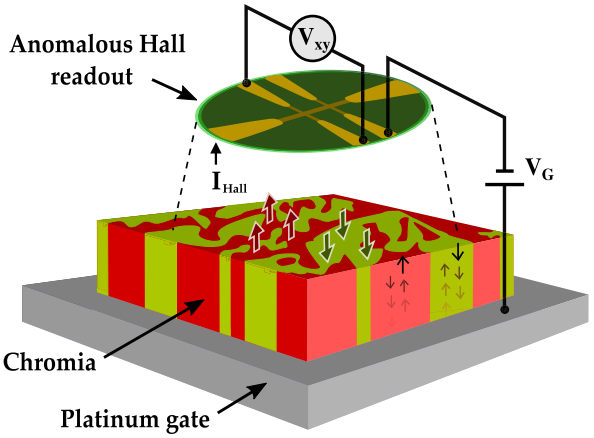


FIGURE 1. Chromia-based magnetoelectric antiferromagnetic random-access memory. Data (1/0) is written by applying a voltage (+/−) to the bottom gate electrode. Read-out is achieved using an anomalous Hall bar electrode placed on top, by applying a Hall bias.

B. ME-AFMRAM : WORKING PRINCIPLE

The chromia-based ME-AFMRAM, which is at the heart of our SMART memory, is shown in Fig. 1. Experimentally demonstrated by Kosub *et al.* [26], the ME-AFMRAM has a bottom gate electrode (Platinum gate in the figure) for applying the gate voltage V_G and providing the necessary electric field to write data into the memory. A small, symmetry-breaking magnetic field (≈ 30 mT) is provided by the stray field of a permanent magnet. A positive voltage V_G will orient the bulk order and, hence, put the surface magnetization in one domain (with surface moments pointing up), whereas a negative voltage will result in the surface magnetization relaxing to the opposite domain (with surface moments pointing down). These two states correspond to binary levels '1' ($V_G > 0$) and '0' ($V_G < 0$), respectively. A gate voltage of 0 V corresponds to the 'hold' mode of the memory cell. Note that the cell serves as non-volatile memory in all gate-voltage ranges, not only for $V_G = 0$.

The read-out is achieved using an anomalous Hall (AH) bar electrode setup, which discerns the boundary magnetization of chromia by sensing the proximity effect-induced magnetization in the nearby Platinum (Pt) electrode, thereby producing a proportional Hall voltage V_{xy} (or V_{AHE}) [27]. Traditionally, the order parameter of AFMs is read-out via an exchange bias arrangement [28] in another FM attached adjacently to the AFM surface. However, the exchange bias and the FM's hysteresis increase the coercive voltage required to overcome the ME barrier and, hence, impact the write energy negatively. To avoid this effect, Kosub *et al.* [26] proposed the use of an exclusively ME-AFM setup with an AH read-out of the surface magnetization, thereby eliminating the need for an FM. At the time of writing this paper, a complete physical understanding of the read-out mechanism for the

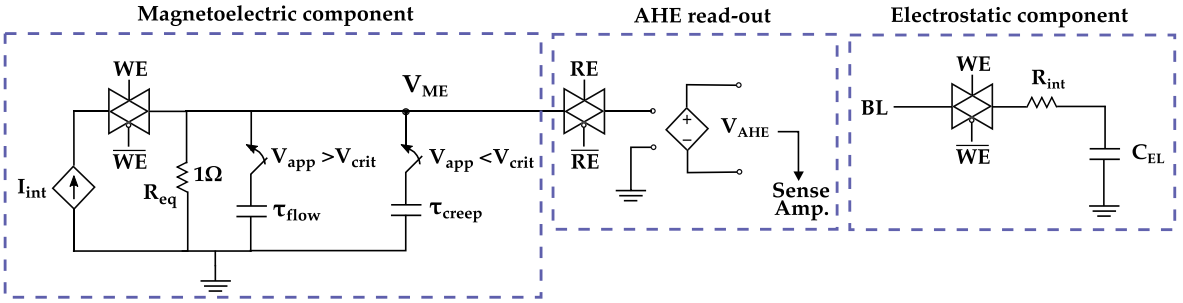


FIGURE 2. Equivalent circuit for the chromia ME-AFMRAM cell. I_{int}, derived from the bit line, writes data on to the node V_{ME}. The time constant of the write operation is τ_{flow} (τ_{creep}) if the applied voltage is greater (smaller) than the critical voltage. Read-out is achieved through an AH setup, modeled with a voltage-controlled voltage source. C_{EL} is the electrostatic capacitance of the chromia dielectric.

boundary magnetization in chromia is lacking. While the authors in [26] have considered an AH-based read-out in their device, recent experiments by C. Binek's group at the University of Nebraska-Lincoln have revealed the contribution of spin-Hall magnetoresistance (SMR) to the read-out signal, which is currently being investigated. However, note that the magnitude of the signal levels is the same in both cases (AH versus SMR) and also the circuit models developed would remain the same, though with different input parameters. For the purposes of this paper, we consider that the read-out signal is due to the AH effect in the proximal heavy metal, as also discussed in prior experimental work.

C. PERFORMANCE MODELING

The ME reversal mechanism in chromia can be classified broadly into two categories, depending on the size of the film compared to the characteristic domain-wall (DW) width. For chromia, the typical DW width $\lambda = \sqrt{A/\mathcal{K}} \sim$ 50-100 nm, where A is the exchange stiffness constant and $\mathcal{K}$ is the uniaxial anisotropy energy [29]. If the sample is much smaller than the DW width, the sample reverses via coherent rotation upon application of the ME pressure. For sample dimension comparable to the DW width, ME reversal occurs via DW nucleation and propagation, which is an incoherent switching process. For both coherent rotation and DW propagation, the reversal could be thermally activated for applied ME pressure lower than the energy barrier between the stable domain states. Otherwise, the domain reversal proceeds in the 'flow' regime [30]. ME-AFMRAM devices currently fabricated have dimensions in the μm range, rendering DW propagation the favorable ME reversal mechanism. To characterize the functionality and performance of chromia ME-AFMRAM, we develop circuit models that represent DW-based reversal in both the thermally activated and the flow regimes. We also provide perspectives and future potential concerning dimensional scaling of the device, which could enable ultra-fast, coherent, rotation-based reversal.

1) DW REVERSAL OF CHROMIA ME-AFMRAM

Consider a chromia sample, where the applied ME pressure creates a pressure difference of $\mathcal{F} = |2\alpha_{ME}EH|$ between the two domains. Here, α_{ME} is the linear ME coefficient.

If $\mathcal{F} > \mathcal{F}_d$ (i.e., for DW de-pinning pressure), the DW propagates as a viscous flow with velocity given as [30]

$$v_{flow} = \frac{\alpha_G \gamma \lambda}{\alpha_+ \xi^2}\left(\frac{\mathcal{F} - \mathcal{F}_d}{M_s}\right)$$

where α_G is the Gilbert damping constant, γ is the gyromagnetic ratio of electron, M_s is the sublattice saturation magnetization, and $\xi = \frac{\alpha_{ME}E}{\mu_0 M_s}$. For a mean free path of l of the DW, the time-scale of ME reversal due to viscous DW propagation is $\tau_{flow} = l/v_{flow}$.

If $\mathcal{F} < \mathcal{F}_d$, the DW undergoes thermal creep to overcome the de-pinning barrier, with a time-scale [30]

$$\tau_{creep} = \sqrt{\frac{\sigma \mathcal{S}^3}{kT}}\left(\frac{\mathcal{F}_d - \mathcal{F}}{2\pi\epsilon}\right)\exp\left[\frac{\mathcal{S}^2(\mathcal{F}_d - \mathcal{F})^2}{4\pi kT\epsilon}\right],$$

where kT is the thermal energy (25 meV at 300 K), ϵ, σ, and $\mathcal{S}$ are the energy, areal density, and surface area, respectively, of the DW. The DW de-pinning pressure is determined by the DW energy, its surface area, and the radius of the non-magnetic de-pinning center.

To write '1' ('0') into the memory cell, a positive (negative) electric field, E_{app}, with a magnitude greater than the critical electric field, E_{crit}, is required, in order to meet the DW propagation criteria of $\mathcal{F} > \mathcal{F}_d$. In this case, the time to write data into the memory is equal to τ_{flow}. When E_{app} is less than E_{crit} (i.e., $\mathcal{F} < \mathcal{F}_d$), the memory cell is in the hold mode and the retention time is specified by τ_{creep}. For typical parameters of chromia, we find $\tau_{creep} \gg \tau_{flow}$, which ensures that the memory cell is thermally stable when it is not accessed. Here, the stability of the cell is determined by τ_{creep}, since longer data retention requires the time constant in the hold mode to be larger. The retention time of the cell can be further improved by enlarging the cell dimensions.

We construct a SPICE circuit model to functionally capture the ME reversal dynamics of chromia. The time constant for reversal of the magnetization of chromia due to an applied ME pressure is represented as $R_{eq} \times C_{eq}$. Without loss of generality, the circuit model uses $R_{eq} = 1\ \Omega$, while C_{eq} is either τ_{flow} or τ_{creep}. To construct the full ME-AFMRAM cell, we combine the RC model of the ME response of chromia with the peripheral read/write circuitry in *Cadence Virtuoso* using the 15-nm CMOS FreePDK technology. Figure 2 shows

TABLE 1. Simulation parameters considered for the ME-AFMRAM cell.

Parameter	Value	Ref.
Saturation magnetization of Cr_2O_3, M_s	2.6×10^5 A/m	[54]
Magnetoelectric coefficient of Cr_2O_3, α_{ME}	3.1×10^{-12} s/m	[55]
Uniaxial anisotropy energy of Cr_2O_3, $\mathcal{K}$	7300 J/m^3	[56]
Gilbert damping constant of Cr_2O_3, α_G	2×10^{-4}	[29]
Threshold ME pressure to depin DW, $\mathcal{F}_d$	25 J/m^3	[30]
Applied magnetic field, H_{app}	0.5 T	
Applied voltage, V_G	0.3 V	
Length of cell, l	60 nm	
Width of cell, w	60 nm	
Thickness of cell, t	10 nm	
Temperature, T	292 K	
τ_{creep} (@ $\mathcal{F} = 0$)	$\sim$ 1 ms	
τ_{flow} (@ $\mathcal{F} = 74.2$ J/m^3)	$\sim$ 0.22 ns	

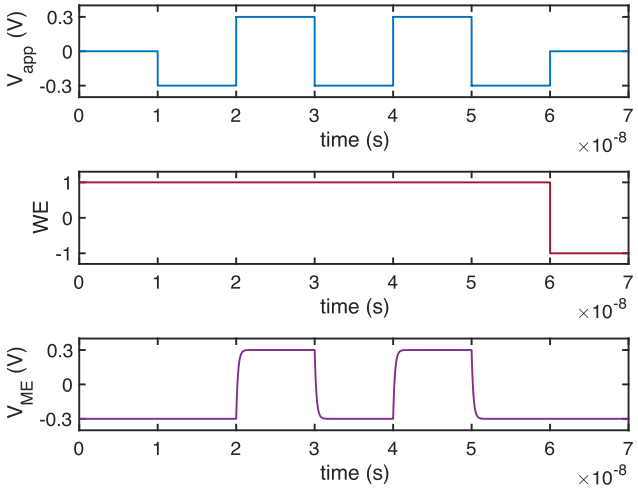


FIGURE 3. Transient simulations showing write operations on the chromia ME-AFMRAM cell. Note that for writing a '1' the write pulse is positive, and for writing a '0' the write pulse is negative. In this simulation, a series of '1's (0.3 V) and '0's (−0.3 V) are being written to the cell, and then finally '0' is retained once Write Enable is switched off.

the equivalent circuit of the ME-AFMRAM cell. The write pulse, used to charge the chromia dielectric and switch its magnetization M, is provided through the current source I_{int} (derived from the bit line) in the write setup. For parameters of chromia listed in Table 1, $C_{flow} = \tau_{flow} \sim 0.223$ nF, $C_{creep} = \tau_{creep} \sim 1$ mF, and $V_{crit} = 0.2$ V. For $|V_G| > 0.2$ V, V_{ME} tracks V_G and data is written into the cell after a write access latency of τ_{flow}. When $|V_G| = 0$ V, data is retained for a time interval of τ_{creep}. Since τ_{creep} is very large, the response in retention/creep mode is extremely slow as compared to write/flow mode. The transient response of the ME-AFMRAM cell is shown in Fig. 3, to highlight the write operation. The write latency of the ME-AFMRAM cell is obtained as $\sim$ 0.63 ns, and the energy-per-bit for one write operation is $\sim$ 0.063 pJ, including the energy required to charge the electrostatic capacitance of chromia. Given relative dielectric permittivity of 11 and dimensions noted in Table 1, the electrostatic capacitance of chromia is calculated as 5.8 aF.

2) ANOMALOUS HALL READ-OUT

To evaluate the read cycle, we set the signals WE to 0 and RE to 1 in Fig. 2. The read setup is designed to sense the boundary magnetization of chromia through an AH arrangement, which transduces the magnetization into a voltage signal. This transduction process is modeled using a voltage-controlled voltage source (VCVS). Typically, a heavy metal such as Pt is used to sense the proximity effect-induced moment from the coupled chromia layer [26].

The AH voltage sensed from the Hall bar arrangement is given as [31]

$$V_{AHE} = \left(\frac{\mu_0 R_s}{t_{Hall}} I_{Hall}\right) M_z,$$

where μ_0 is the vacuum permeability, R_s is the AH coefficient, I_{Hall} is the Hall bias current, t_{Hall} is the thickness of the Hall layer and M_z is the proximity effect-induced magnetization. In the case of Pt/Cr_2O_3, R_s is only about $\sim$ 5 pΩm/T for $t_{Pt} = 10$ nm and $T = 300$ K [32]. This results in an AH signal $V_{AHE} \sim 0.3$ μV, considering a Hall bias of 2 mA and a magnetoelectric node voltage $V_{ME} = 0.3$ V. The Hall signal can be raised to ~ 1 μV by increasing V_{app} to 1 V, and further enhanced by applying a larger Hall bias. However, doing so would negatively impact the energy consumed in the read operation. Sensing such a low μV-range AH signal would require sophisticated instrumentation sense amplifiers that are area- and power-prohibitive (e.g., 2.5 mm^2 area and ∼mW-range power [33]).

This problem can be addressed by exploring other material systems with much higher interfacial spin-orbit coupling (SOC), resulting in larger AH coefficients. In [34], a Pt/Co/Pt tri-layer is shown to exhibit $R_s \sim 7.3 \times 10^{-10}$ Ωm/T at 300 K for $t_{Co} \sim 10$ nm, resulting in $V_{AHE} \sim 43.8$ μV at a Hall bias of 2 mA and $V_{ME} = 0.3$ V. Magnetic semiconductors like $EuTiO_3$ possess higher $R_s \sim 8 \times 10^{-9}$ Ωm/T for $t_{EuTiO_3} = 25$ nm [35]. However, AH signals in such samples have been detected only at very low temperatures, of 2K, at which the ME effect in Cr_2O_3 vanishes. The Hall signal could be improved in a topological insulators (TI) due to the presence of high SOC-enhanced surface states. For example, the $Bi_2Se_3/LaCoO_3$ stack considered in [36] demonstrates R_s as high as ~ 1.59 μΩm/T at 100 K for $t_{Bi_2Se_3} \sim 20$ nm. This results in a substantial improvement in the AH signal generated (i.e., $\sim$ 47.7 mV). The AH effect in the $Bi_2Se_3/LaCoO_3$ interface is ascribed to the exchange coupling between the Bi_2Se_3 layer and the ferromagnetic $LaCoO_3$ layer via the proximity effect, and is enhanced by the high interfacial SOC. Similarly, the $(BiSb)_2Te_3$/TIG system considered in [37] achieves a mV-range AH signal, though much closer to room temperature. A comparison of R_s/t in various material systems is illustrated in Fig. 4. As can be inferred, TIs are an ideal material candidate to implement the AH read-out layer with

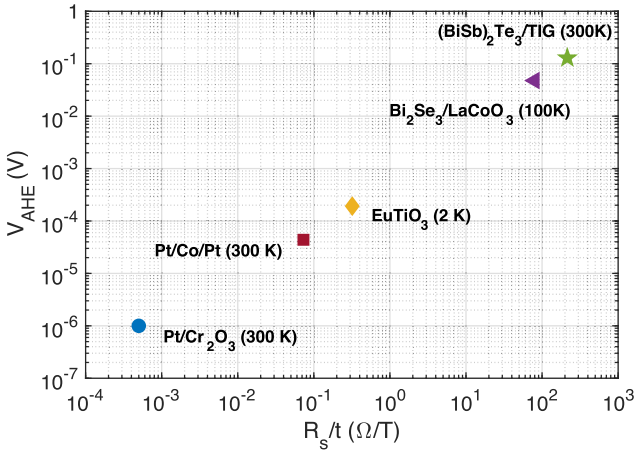


FIGURE 4. Comparison of the AH coefficient per unit thickness and AH signal magnitude in different material systems. The AH signal V_{AHE} is calculated for a Hall bias of 2 mA and a magnetoelectric node voltage $V_{ME} \sim 0.3$ V. TIs with high interfacial SOC exhibit greater AH coefficients and can generate large AH signals, capable of being detected by conventional current sense amplifiers.

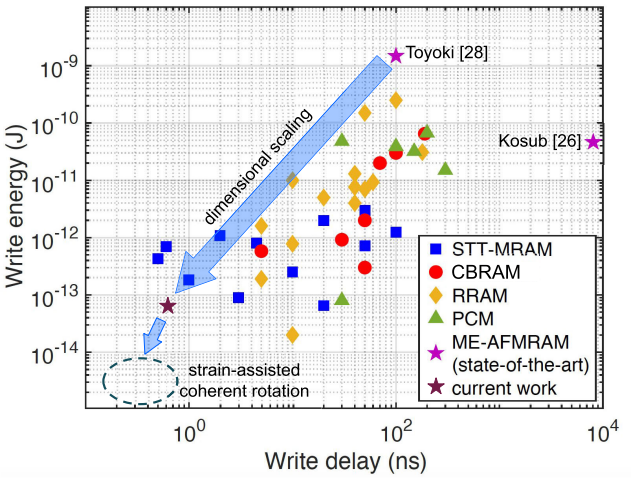


FIGURE 5. Benchmarking the ME-AFMRAM cell considered in this work against current state-of-the-art ME-AFMRAM technology, and trends in other emerging non-volatile storage devices from [39]. Some important data points in this plot, representing the advances in various NVMs, include [40]–[42] for STT-MRAM, [43]–[45] for CBRAM, [46]–[48] for RRAM, and [49]–[51] for PCM, respectively. The future potential of ME-AFMRAM lies in achieving ultra-fast, coherent rotation-based reversal (sub-100 ps write delay and fJ write energy) through a combination of dimensional scaling and strain-augmentation.

Cr_2O_3 due to the potential of a ∼mV-range AH signal, which can be easily read-out using a normal current latch sense amplifier [38], i.e., without the need for sophisticated sensing equipment.

3) COHERENT ROTATION-BASED REVERSAL

The ∼ns-range write latency of the ME-AFMRAM cell can be improved drastically if the chromia order can be switched through coherent rotation. In this case, the entire chromia sample undergoes reversal homogeneously, rather than following the incoherent DW propagation. For $\mathcal{F}_d > 4\mathcal{K}$, the order parameter switches via damping of gyromagnetic precessions [30]. However, if $\mathcal{F}_d < 4\mathcal{K}$, magnetization could switch due to thermal activation. Here, the switching time is exponentially dependent on the energy barrier of the sample. In any case, it is thermal activation that leads to retention errors.

To realize coherent rotation in chromia, the applied ME pressure must exceed $4\mathcal{K} = 2.92 \times 10^4$ J/m^3. For a magnetic field of 0.5 T and $\alpha_{ME} = 3.1$ ps/m, the electric field required for coherent rotation is 1.18×10^{10} V/m. Unfortunately, such a high electric field could lead to dielectric breakdown of chromia, given that the breakdown strength of chromia is $\sim 2 \times 10^8$ V/m [52]. A potential solution to this challenge is to reduce the effective anisotropy of the sample such that the required threshold electric field scales down. This can be achieved through a variety of techniques, including substitutional alloying and the application of mechanical strain [53]. It is estimated that the write latency of a strain-augmented ME-AFMRAM cell can reach as low as a few 10's of ps. A comparison of the current state-of-the-art in ME-AFMRAM technology and its future potential versus trends in other emerging storage devices is presented in Fig. 5.

4) MATERIAL AND GEOMETRICAL PARAMETERS OF THE CHROMIA ME-AFMRAM CELL

The simulation parameters used in our SPICE models for the chromia ME-AFMRAM are listed in the following Table 1.

D. ME-AFMRAM ARRAY

To evaluate the system-level performance of ME-AFMRAM in the context of existing memory technologies, we simulate a 64KB DW-based ME-AFMRAM chip on NVSim, a standard tool for estimating the performance metrics of emerging NVMs [57]. The organization of this 64KB memory, as leveraged from [57], is shown in Fig. 6. The internal architecture of the ME-AFMRAM cell array, along with the peripheral decoders, drivers and sense amplifiers, constructed at the 15-nm CMOS node, is highlighted in Fig. 7. The total write latency of the 64KB ME-AFMRAM, including the parasitics and peripheral latency (133.9 ps) and the dominant cell switching time (∼630 ps), is obtained as 763.9 ps from NVSim [57]. The write latency can be improved by an order of magnitude via coherent rotation of the order parameter. The total read latency of the chip, obtained from NVSim [57], is ∼2.3 ns. This includes contributions from the sense amplifier (1.45 ns), bit-line parasitics (3.5 ps), decoders and other peripherals (∼150 ps), and the AH measurement delay in the Bi_2Se_3 layer (∼0.7 ns) [63]. State-of-the-art pulsed AH measurement schemes like [63] are capable of operating in the GHz regime.

The output bit-line sensing can be achieved using a conventional current latch amplifier if a large-SOC material such as a TI is used to generate an AH signal in the range of tens of mV. The read/write endurance of the ME-AFMRAM is

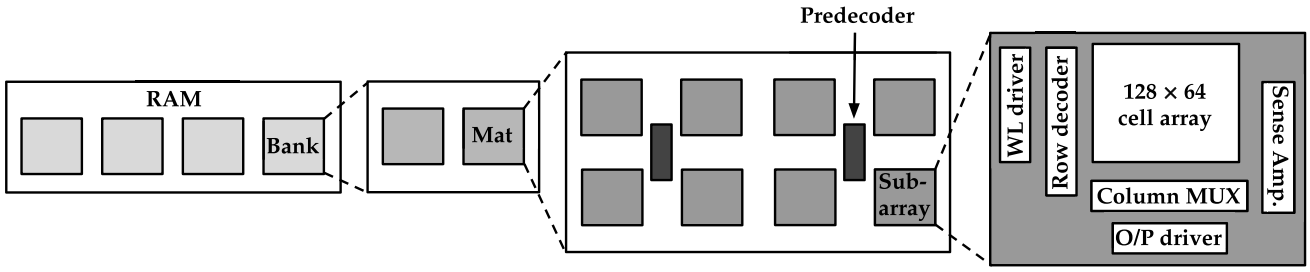


FIGURE 6. 64KB ME-AFMRAM organization with 4 × 1 banks, 2 × 1 mats, 4 × 2 sub-arrays, and 128 × 64 bit cell arrays. Here, the word length is 128 bit. The memory organization is leveraged from [57].

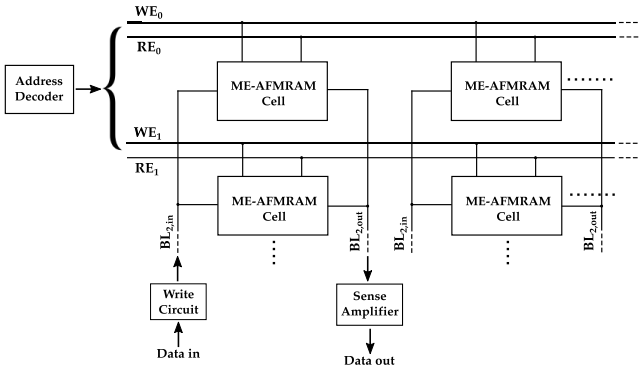


FIGURE 7. Construction of the ME-AFMRAM cell array used in the memory architecture. The signals $BL_{i,in}$ serve to write data into the cells when Write Enable (WE) is on, and signals $BL_{i,out}$ serve to read data from the cells when Read Enable (RE) is on.

TABLE 2. Performance comparison of various memory technologies, from [58]–[62]. The write and read latencies for ME-AFMRAM (DW model) are quoted for a 64KB memory with a 128-bit word line, simulated using NVSim [57]. The energy-per-bit metric is for a single bit write onto a cell.

Memory technology	Write latency	Read latency	Energy-per-bit	Endurance (cycles)	Reciprocal density	Ref.
DRAM	10 ns	10 ns	3 pJ	10^{16}	6 - 12 F^2	[58]
NAND Flash	220 µs	25 µs	300 pJ	10^4	1 - 4 F^2	[59]
PCM	50 ns	10 ns	2 pJ	10^8	4 - 16 F^2	[58]
FeRAM	60 ns	60 ns	2.5 pJ	10^{13}	12 F^2	[60]
ReRAM	30 ns	20 ns	0.4 pJ	10^5	4 F^2	[61]
Memristor	10 ns	10 ns	0.1 pJ	10^{12}	4 F^2	[58]
STT-MRAM	2-10 ns	2-10 ns	0.1 pJ	10^{15}	20 - 60 F^2	[62]
ME-AFMRAM	764 ps	2.3 ns	0.063 pJ	10^{15}	4 - 16 F^2	

expected to be similar to that of STT-MRAM. A comparison of the performance metrics of the ME-AFMRAM with other memory technologies at the chip-level is presented in Table 2. It can be seen that the ME-AFMRAM offers some competitive advantages over other NVMs as well as over conventional memory systems.

III. APPLICATION AS SECURE MEMORY

After conducting cell- and array-level modeling and benchmarking of the chromia-based ME-AFMRAM, we continue with the implementation of the proposed SMART memory using the ME-AFMRAM.

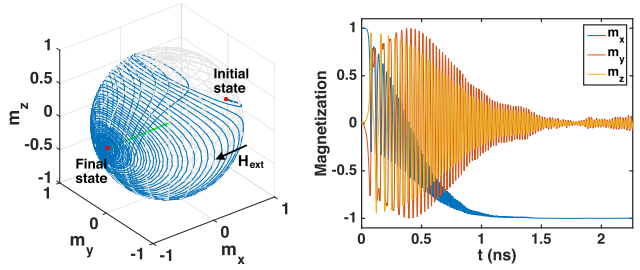
A. THREAT MODEL

First, we discuss the threat model, defining the strengths and capabilities of attackers, as well as the objectives and consequences of a successful attack. Most but not all attack scenarios presented here are specific to NVMs.

- Attackers can launch cold-boot attacks [9]. During power-down, there is some latency after the power-down sequence initiates until the moment when memory contents are completely secured. An attacker might use this gap to read out memory contents. To circumvent such attacks, memory encryption is typically employed [12], [16].
- Attackers could leverage properties like sensitivity to magnetic fields and temperature fluctuations to corrupt the data or induce a DoS [11]. They may forcibly write specific data patterns to memory, which accelerates aging and causes memory failures.
- With access to failure analysis equipment, attackers can also resort to advanced invasive attacks. The majority of such attacks target at the back-end-of-line (BEOL), approaching from the top-most metal layer, which is also referred to as front-side attacks. Various countermeasures have been proposed to protect the front-side, which include protective meshes, shields, and sensors [64], [65]. In any case, *bus snooping* attacks are considered beyond the scope of this work.
- Power-dissipation signatures when reading/writing '0' and '1' within the NVM can be exploited for side-channel attacks to infer the data, through techniques like differential power analysis (DPA) [66] and correlation power analysis (CPA) [67].

B. MAGNETIC FIELD AND TEMPERATURE ATTACKS

STT-MRAMs have FM-based MTJs as their basic building blocks. FMs possess a macroscopic magnetization (or



(a) Trajectory for magnetic field-induced switching of a FM.

(b) Components for magnetic field-induced switching of a FM.

FIGURE 8. The FMs in an STT-MRAM can be switched easily using external magnetic fields.

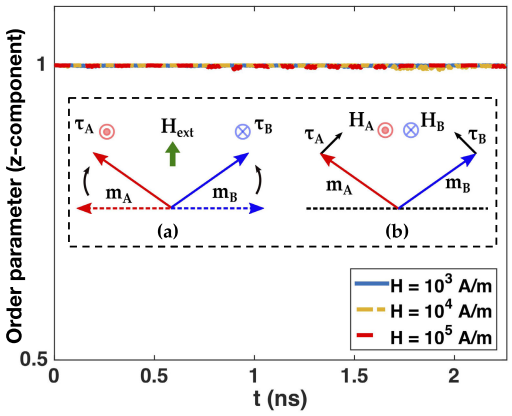


FIGURE 9. The application of a magnetic field is unable to switch the AFM order parameter, even when increasing the field magnitude. Inset: (a) an external, homogeneous magnetic field may cant the sublattice moments, but it is incapable of rotating the AFM order; (b) staggering fields on the sublattice moments produce staggered tangential torques, which can reorient the AFM order.

magnetic signature) that can be probed or inferred with using an external magnetic field. Hence, magnetic fields can be used to infer or tamper with the stored data or even cause malfunctions in STT-MRAMs [11]. Stray magnetic fields as small as 10 mT could cause an unintended bit flip in STT-MRAM cells. Figure 8 shows the magnetic field-induced bit flip in a representative FM, obtained by solving the Landau-Lifshitz-Gilbert equation for the FM dynamics [68].

AFMs, on the other hand, exhibit no external magnetic signature since their equal and opposite sublattice moments cancel each other out. Hence, the bulk order parameter cannot be affected by external magnetic fields. To switch the bulk order, staggered fields (opposite sign on opposite sublattices) must be applied on both the sublattice moments, as illustrated in Fig. 9 inset. However, an external, homogeneous magnetic field is unable to provide such a staggered field arrangement, and hence, ends up canting the sublattice moments in a way wherein the torque due to the external field is exactly balanced by the exchange torque exerted by one sublattice moment on the other [69]. Since external magnetic fields are unable to reorient the AFM order parameter, the SMART ME-AFMRAM is expected to be resistant to magnetic field attacks described in [11]. We note that switching the ME-AFM surface magnetization state using a combination of E and H fields would require an exact knowledge of the write cycles and the prior state of the surface, as well as means to control the electric field explicitly, which is to be concealed from an attacker.

With regards to temperature fluctuation-based attacks, an adversary might increase the ambient temperature of the ME-AFMRAM in an attempt to alter the stored data. Note that the Néel temperature of pure chromia is 308 K [70], above which the AFM ordering is destroyed. Hence, the attacker may corrupt the memory by heating it above the Néel temperature. To counter this, we consider Boron-doped chromia, whose Néel temperature is demonstrated experimentally to be $\sim$ 400 K [71]. Hence, Boron-doped chromia can increase the resilience of SMART memory against temperature fluctuations. That is because such larger temperature fluctuations (above 400 K) are easier to detect, and countermeasures like interception of such attacks become more feasible.

C. DATA CONFIDENTIALITY ATTACKS

As with all NVMs, data remanence in the SMART memory could be exploited by attackers to steal sensitive information. The most effective countermeasure against such data confidentiality attacks, including cold-boot and stolen memory-modules attacks, is to encrypt the data using a secure encryption scheme before storing it in the memory. Advanced memory encryption techniques like counter mode encryption (CME) use block ciphers such as Advanced Encryption Standard (AES) to encrypt a seed using a secret key, in order to generate a one-time pad (OTP). The seed for each write on a memory line consists of a secret key, the line address, and a counter value associated with that line, which is incremented with each subsequent write to the same line. Hence, the generated OTP is unique for each line address, and also for each write operation to the same address. The OTP is then XOR-ed with the plaintext to obtain the ciphertext, which is stored in the non-volatile main memory. Note that the secret key used in the AES core is considered inaccessible to the attacker.

Directly applying XOR-based CME scheme to the SMART memory would result in large encryption overheads. This is because the CME scheme is tailored for NVMs like PCM and STT-MRAM, whose write time is on the order of $\sim$ns. The access latency of ME-AFMRAM is sub-ns for DW-based propagation and few 10's of ps for coherent rotation. A general encryption scheme for SMART memory, switching either via DW propagation or coherent rotation, must be such that the overall memory access latency is not adversely affected. Existing encryption solutions based on CMOS XOR gates with 10's of ps delay are rendered ineffective as their encryption time is comparable to the memory write time, resulting in idle clock cycles.

Here, we propose to use in-memory encryption, or *Memcryption*, using bitwise CNOT (i.e., controlled-NOT) gates constructed from ME-AFM-based logic. By tying the

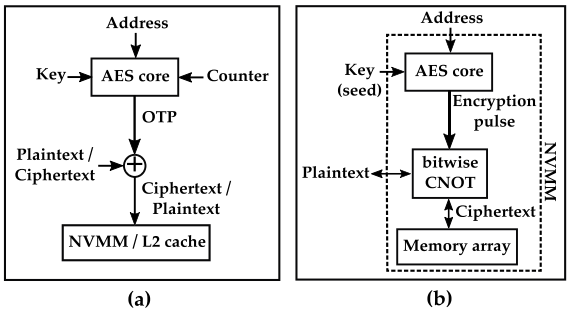


FIGURE 10. (a) CME uses AES to generate an OTP, using the memory line address, a counter, and a secret key. The encryption and decryption is performed outside the non-volatile main memory (NVMM). (b) *Memcryption* uses a secret key and the line address as seed for AES, to generate an encryption pulse. That pulse is used to control the bitwise operation of CNOT gates, and is embedded in the data path within the NVMM.

encryption pulse to the control signals of CNOT gates, one can achieve such *Memcryption*. Spin devices like the ME-AFM transistor [72] are able to implement polymorphic logic gates, which can provide inverting or non-inverting functionality based on a control signal [73], [74]. Hence, the ME-AFM transistor is used to realize the CNOT gate. Further, the ME-AFM transistor is shown to exhibit delays as small as $\sim$ 10 ps, which is substantially faster than CMOS XOR gates and compatible with the SMART memory write-times. Such homogeneity in the technology and materials by using only ME-AFM for both the memory cells and the CNOT gates will ease the fabrication. In *Memcryption*, we embed ME-AFM transistor-based CNOT gates directly in the data path connected to the memory array; hence, the encryption is in-memory, as opposed to prior works using a separate encryption block. This integration of encryption and memory array is not detrimental to the memory density since ME-AFM transistors have a footprint that is substantially smaller than that of CMOS XOR gates. Figure 10 contrasts our *Memcryption* scheme with prior CME techniques.

The SMART memory architecture with *Memcryption* is shown in Fig. 11. A trusted 128-bit key, provided and stored within a secure processing module (SPM) along with the processor, is concatenated with the memory address and used as seed for AES. The AES core, which is to be integrated on the NVM chip,[1] thus produces an encryption pulse whose bits are used as the control bits for the CNOT gates of the in-memory encryption layer. Depending on the control bits, the encryption layer flips bits selectively in the plaintext before performing a memory-write. During decryption, the same encryption pulse is generated again and used to perform bit-wise CNOT operations on the ciphertext (read from memory), to obtain the plaintext.

A comparison of the *Memcryption* scheme versus CME (when also applied to ME-AFMRAM) is presented in Table 3.

[1]Heterogeneous spin-CMOS integration is not prohibitive since the underlying AFM technology is compatible with CMOS processes in the BEOL. In general, hybrid spin-CMOS designs have been explored in prior works [75].

The array considered is a 128-bit ME-AFMRAM, while the AES and CMOS peripherals are synthesized using the 15nm *NanGate* technology. We observe that Memcryption with SMART memory has a better encryption latency than CME, which utilizes regular CMOS XORs. We also note that *Memcryption* helps reduce the encryption latency but is similar to CME with respect to the energy overheads. That is because energy dissipation is dominated by the AES core in any case. We also reiterate that *Memcryption* is tailored specifically as a memory-side scheme for ME-AFMRAM, to achieve low encryption latency, owing to the homogeneous delays of the memory array and the encryption layer. However, it may not serve well as an efficient implementation for any generic NVM.

With regards to the reliability and lifetime of the ME-AFMRAM used to construct the SMART memory, its endurance is comparable to that of STT-MRAM. However, it also suffers from the same errors that plague the STT-MRAM, i.e., faults in the peripheral CMOS circuitry including the access transistors [76]. To address these faults and ensure the correctness of the stored data, standard error correction techniques for NVMs [77] like the error correction pointer (ECP) and other advanced schemes based on ECP, including "Pay-As-You-Go" [78] and "Zombie memory" [79], can be implemented memory-side and integrated on the ME-AFMRAM array. The ECP memory can be realized using homogeneous spintronics technology, including the STT-MRAM or the ME-AFMRAM itself, or by leveraging heterogeneous spin-CMOS integration.

D. POWER SIDE-CHANNEL ATTACKS

Asymmetric read/write characteristics in NVMs like STT-MRAM make them susceptible to side-channel attacks which exploit the different signatures incurred when reading/writing '1's and '0's bits. STT-MRAMs employ MTJs with a fixed FM reference layer, with another free layer either oriented parallel or anti-parallel to that reference layer. Depending on the relative orientation of these two layers, the MTJ falls into a low or high resistance state; the low or high state corresponds to logic '0' or logic '1' state, respectively. Hence, the currents drawn for read/write operations are different depending on reading/writing a '0' or a '1'. Thus, an attacker could attach a resistor in a voltage-divider configuration with the MTJ cell, monitor the voltage drops across that resistor, and perform DPA to recover the data being written to or read from the cell. In fact, such an attack was showcased against an STT-MRAM-based cache in [81].

For the SMART memory, recall that writing is achieved using electrical fields, not currents. Further, the electric-field magnitude required for writing '0's and '1's is equivalent; see write voltage and polarization voltage traces in Fig. 3. This is because there is no reference layer or tunneling magnetoresistance in the ME-AFMRAM, which would cause asymmetricity. As for the read operation, the proximity effect-induced moment in the Pt electrode is slightly different for reading '0' or '1'. However, this imbalance in the Hall signals can

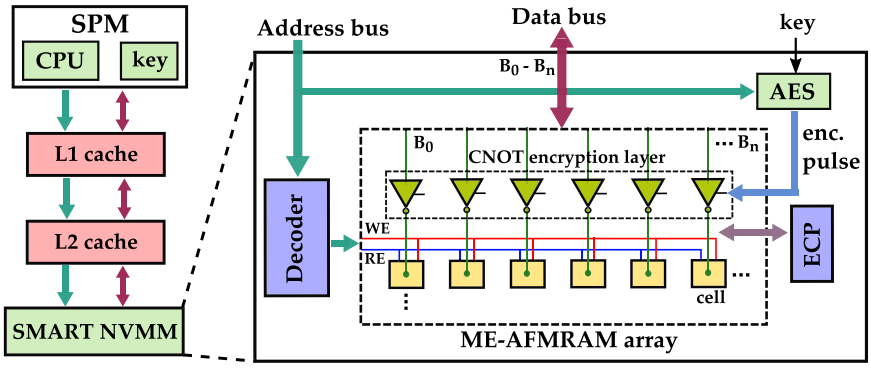


FIGURE 11. SMART memory architecture with *Memcryption*. The CNOT layer for decryption is not shown for simplicity.

TABLE 3. Comparison for latency and energy when applying the CME and *Memcryption* schemes to a 128-bit ME-AFMRAM array. The baseline latency for the unencrypted array is ∼ 100 ps.

Encryption technique	Latency	Energy
CME [80]	299.23 ps (2.99×)	17.371 pJ
Memcryption	273.46 ps (2.73×)	17.370 pJ

be compensated for by introducing appropriate offsets in the Hall measurement setup, as demonstrated in [26]. Hence, the SMART memory can achieve symmetric signatures for both read and write and for both '0→1' and '1→0' transitions, thus thwarting any DPA-based power side-channel attacks.

E. PHOTONIC SIDE-CHANNEL AND BACKSIDE ATTACKS

Leveraging the photonic side-channel (PSC) to circumvent the security guarantees provided by cryptographic algorithms like AES and RSA has been demonstrated recently [82], [83]. Simple Photonic Emission Analysis (SPEA) or Differential Photonic Emission Analysis (DPEA) can be carried out using photo-emission equipment available for similar cost as that of power-analysis equipment. The essence of the PSC is to observe photo-emissions emanating for switching of CMOS transistors. For SRAM- or DRAM-based memories, this emission can then be correlated with the data being programmed into the memory. In [82], the PSC was found to originate when kinetic energy gained by charge carriers in the transistor channel is transferred to photons, which are visible through photo-detectors. In [83], the authors leveraged this information to perform a side-channel attack, ultimately recovering the full AES key. Modern-day chips use several metal layers, which interfere with the emission of photons from the frontside of any integrated circuit (IC); therefore, a natural direction is to observe the photon emission from the backside of ICs.

While CMOS-based memory technologies like SRAM and DRAM are prone to such PSC attacks, the SMART memory is AFM-based and involves no photonic emissions emanating from transistor channels. Data read-out in the SMART memory can only be accomplished through an AH measurement setup. Further, even if an advanced attacker is able to isolate the SMART memory cell and gain access to the AH setup from the frontside, they would only be able to recover the encrypted ciphertext (as described in Sec. III-C).

IV. CONCLUSION

In this paper, we present *SMART: A Secure Magnetoelectric Antiferromagnet -Based Tamper-Proof Non-Volatile Memory*, by utilizing the unique properties of ME-AFMs. The ME-AFMRAM, which is at the core of the SMART memory, has an access latency of sub-1 ns (for DW-based switching) down to only 10's of ps (for coherent rotation switching) with an energy-per-bit of ∼ 0.13 pJ. Besides its superior performance as compared to prior NVMs like STT-MRAM and PCM, the SMART memory exhibits no sensitivity to external magnetic fields, which makes it resilient to magnetic field-based data tampering and denial of memory service attacks that commonly plague other ferromagnets-based NVMs. To solve the security vulnerability of data remanence (after power-down) in the SMART memory, we demonstrate a new encryption technique called *Memcryption*. This scheme employs emerging ME-AFM-based logic to implement a CNOT-centric in-memory encryption, which is particularly tailored to reduce the encryption and decryption latency in the SMART memory. Further, symmetric read and write signatures for '0' and '1' bits render prominent side-channel attacks like the differential power attack futile against the SMART memory. Advanced photonic side-channel attacks, which are powerful threats against any CMOS IC by observing all internal transistor activity from the frontside or backside, are ineffective against the SMART memory due to the fundamentally different switching mechanism as well as the proposed *Memcryption* safeguard.

REFERENCES

[1] S.-K. Park, "Technology scaling challenge and future prospects of DRAM and NAND flash memory," in *Proc. IEEE Int. Memory Workshop (IMW)*, May 2015, pp. 1–4.

[2] H. Wang, K. Zhao, M. Lv, X. Zhang, H. Sun, and T. Zhang, "Improving 3D DRAM fault tolerance through weak cell aware error correction," *IEEE Trans. Comput.*, vol. 66, no. 5, pp. 820–833, May 2017.

[3] Y. Kim, "Architectural techniques to enhance DRAM scaling," Ph.D. dissertation, Dept. Elect. Comput. Eng., Carnegie Mellon Univ., Pittsburgh, PA, USA, 2015.
[4] O. Mutlu, "Main memory scaling: Challenges and solution directions," in *More Than Moore Technologies for Next Generation Computer Design*. New York, NY, USA: Springer, 2015, pp. 127–153.
[5] E. Wyrwas, "Proton irradiation of the 16 GB Intel Optane SSD," NASA Goddard Space Flight Center, Greenbelt, MD, USA, Tech. Rep. TN49014-TR-17-045, 2017.
[6] *16 Mb 256 K × 16 MRAM Memory—Everspin*. Accessed: Nov. 20, 2018. [Online]. Available: https://www.everspin.com/file/882/download
[7] P. Kocher, J. Horn, A. Fogh, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom, "Spectre attacks: Exploiting speculative execution," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2019, pp. 1–19.
[8] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, A. Fogh, J. Horn, S. Mangard, P. Kocher, and D. Genkin, "Meltdown: Reading kernel memory from user space," in *Proc. 27th USENIX Secur. Symp. (USENIX Secur.)*, 2018, pp. 973–990.
[9] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten, "Lest we remember: Cold-boot attacks on encryption keys," *Commun. ACM*, vol. 52, no. 5, pp. 91–98, May 2009.
[10] V. Young, P. J. Nair, and M. K. Qureshi, "DEUCE: Write-efficient encryption for non-volatile memories," *ACM SIGARCH Comput. Archit. News*, vol. 43, no. 1, pp. 33–44, 2015.
[11] J.-W. Jang, J. Park, S. Ghosh, and S. Bhunia, "Self-correcting STTRAM under magnetic field attacks," in *Proc. 52nd Annu. Design Autom. Conf. (DAC)*, 2015, pp. 1–6.
[12] S. Chhabra and Y. Solihin, "i-NVMM: A secure non-volatile main memory system with incremental encryption," in *Proc. 38th Annu. Int. Symp. Comput. Archit. (ISCA)*, Jun. 2011, pp. 177–188.
[13] S. Kannan, N. Karimi, and O. Sinanoglu, "Secure memristor-based main memory," in *Proc. 51st ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, Jun. 2014, pp. 1–6.
[14] A. K. Mandal, C. Parakash, and A. Tiwari, "Performance evaluation of cryptographic algorithms: DES and AES," in *Proc. IEEE Students' Conf. Electr., Electron. Comput. Sci.*, Mar. 2012, pp. 1–5.
[15] S. Swami, J. Rakshit, and K. Mohanram, "SECRET: Smartly EnCRypted energy efficient non-volatile memories," in *Proc. 53rd Annu. Design Autom. Conf. (DAC)*, 2016, pp. 1–6.
[16] S. Swami and K. Mohanram, "ACME: Advanced counter mode encryption for secure non-volatile memories," in *Proc. 55th ACM/ESDA/IEEE Design Autom. Conf. (DAC)*, Jun. 2018, pp. 1–6.
[17] G. T. Rado and V. J. Folen, "Observation of the magnetically induced magnetoelectric effect and evidence for antiferromagnetic domains," *Phys. Rev. Lett.*, vol. 7, no. 8, pp. 310–311, Oct. 1961.
[18] R. Khymyn, I. Lisenkov, V. Tiberkevich, B. A. Ivanov, and A. Slavin, "Antiferromagnetic THz-frequency Josephson-like oscillator driven by spin current," *Sci. Rep.*, vol. 7, no. 1, May 2017, Art. no. 43705.
[19] A. K. Agyei and J. L. Birman, "On the linear magnetoelectric effect," *J. Phys., Condens. Matter*, vol. 2, no. 13, pp. 3007–3020, Apr. 1990.
[20] W. Echtenkamp and C. Binek, "Electric control of exchange bias training," *Phys. Rev. Lett.*, vol. 111, no. 18, Oct. 2013, Art. no. 187204.
[21] N. Wu, X. He, A. L. Wysocki, U. Lanke, T. Komesu, K. D. Belashchenko, C. Binek, and P. A. Dowben, "Imaging and control of surface magnetization domains in a magnetoelectric antiferromagnet," *Phys. Rev. Lett.*, vol. 106, no. 8, Feb. 2011, Art. no. 087202.
[22] X. He, Y. Wang, N. Wu, A. N. Caruso, E. Vescovo, K. D. Belashchenko, P. A. Dowben, and C. Binek, "Robust isothermal electric control of exchange bias at room temperature," *Nature Mater.*, vol. 9, no. 7, pp. 579–585, Jul. 2010.
[23] L. Fallarino, A. Berger, and C. Binek, "Magnetic field induced switching of the antiferromagnetic order parameter in thin films of magnetoelectric chromia," *Phys. Rev. B, Condens. Matter*, vol. 91, no. 5, Feb. 2015, Art. no. 054414.
[24] C. Brown and T. O'Dell, "Domain switching measurements in an antiferromagnet," *IEEE Trans. Magn.*, vol. MAG-5, no. 4, pp. 964–967, Dec. 1969.
[25] T. J. Martin, "Antiferromagnetic domain switching in Cr_2O_3," *Phys. Lett.*, vol. 17, no. 2, pp. 83–85, Jul. 1965.
[26] T. Kosub, M. Kopte, R. Hühne, P. Appel, B. Shields, P. Maletinsky, R. Hübner, M. O. Liedke, J. Fassbender, O. G. Schmidt, and D. Makarov, "Purely antiferromagnetic magnetoelectric random access memory," *Nature Commun.*, vol. 8, no. 1, Apr. 2017, Art. no. 13985.
[27] T. Kosub, M. Kopte, F. Radu, O. G. Schmidt, and D. Makarov, "All-electric access to the magnetic-field-invariant magnetization of antiferromagnets," *Phys. Rev. Lett.*, vol. 115, no. 9, Aug. 2015, Art. no. 097201.
[28] K. Toyoki, Y. Shiratsuchi, A. Kobane, C. Mitsumata, Y. Kotani, T. Nakamura, and R. Nakatani, "Magnetoelectric switching of perpendicular exchange bias in Pt/Co/α-Cr_2O_3/Pt stacked films," *Appl. Phys. Lett.*, vol. 106, no. 16, Apr. 2015, Art. no. 162404.
[29] K. D. Belashchenko, O. Tchernyshyov, A. A. Kovalev, and O. A. Tretiakov, "Magnetoelectric domain wall dynamics and its implications for magnetoelectric memory," *Appl. Phys. Lett.*, vol. 108, no. 13, Mar. 2016, Art. no. 132403.
[30] A. Parthasarathy and S. Rakheja, "Dynamics of magnetoelectric reversal of an antiferromagnetic domain," *Phys. Rev. A, Gen. Phys.*, vol. 11, no. 3, Mar. 2019, Art. no. 034051.
[31] R. A. Griffiths, "Anomalous Hall effect measurements of bilayer magnetic structures," Ph.D. dissertation, Univ. Manchester, Manchester, U.K., 2017.
[32] S. Meyer, R. Schlitz, S. Geprägs, M. Opel, H. Huebl, R. Gross, and S. T. B. Goennenwein, "Anomalous Hall effect in YIG|Pt bilayers," *Appl. Phys. Lett.*, vol. 106, no. 13, Mar. 2015, Art. no. 132402.
[33] J. F. Witte, J. H. Huijsing, and K. A. Makinwa, "A current-feedback instrumentation amplifier with 5μV offset for bidirectional high-side current-sensing," *IEEE J. Solid-State Circuits*, vol. 43, no. 12, pp. 2769–2775, 2008.
[34] P. Zhang, W. Lin, D. Wu, Z. Jiang, and H. Sang, "Effective anomalous Hall coefficient in an ultrathin Co layer sandwiched by Pt layers," *J. Appl. Phys.*, vol. 115, no. 6, Feb. 2014, Art. no. 063908.
[35] K. S. Takahashi, H. Ishizuka, T. Murata, Q. Y. Wang, Y. Tokura, N. Nagaosa, and M. Kawasaki, "Anomalous Hall effect derived from multiple Weyl nodes in high-mobility $EuTiO_3$ films," *Sci. Adv.*, vol. 4, no. 7, Jul. 2018, Art. no. eaar7880.
[36] S. Zhu, D. Meng, G. Liang, G. Shi, P. Zhao, P. Cheng, Y. Li, X. Zhai, Y. Lu, L. Chen, and K. Wu, "Proximity-induced magnetism and an anomalous Hall effect in Bi_2Se_3/$LaCoO_3$: A topological insulator/ferromagnetic insulator thin film heterostructure," *Nanoscale*, vol. 10, no. 21, pp. 10041–10049, 2018.
[37] C. Tang, C.-Z. Chang, G. Zhao, Y. Liu, Z. Jiang, C.-X. Liu, M. R. McCartney, D. J. Smith, T. Chen, J. S. Moodera, and J. Shi, "Above 400-K robust perpendicular ferromagnetic phase in a topological insulator," *Sci. Adv.*, vol. 3, no. 6, Jun. 2017, Art. no. e1700307.
[38] T. Kobayashi, K. Nogami, T. Shirotori, and Y. Fujimoto, "A current-controlled latch sense amplifier and a static power-saving input buffer for low-power architecture," *IEEE J. Solid-State Circuits*, vol. 28, no. 4, pp. 523–527, Apr. 1993.
[39] H. Wong, C. Ahn, J. Cao, H. Chen, S. Fong, Z. Jiang, C. Neumann, S. Qin, J. Sohn, and Y. Wu, "Stanford memory trends," Stanford Univ., Stanford, CA, USA, Tech. Rep., 2016.
[40] G. Jan, Y.-J. Wang, T. Moriyama, Y.-J. Lee, M. Lin, T. Zhong, R.-Y. Tong, T. Torng, and P.-K. Wang, "High spin torque efficiency of magnetic tunnel junctions with MgO/CoFeB/MgO free layer," *Appl. Phys. Exp.*, vol. 5, no. 9, Sep. 2012, Art. no. 093008.
[41] M. Gajek, J. J. Nowak, J. Z. Sun, P. L. Trouilloud, E. J. O'Sullivan, D. W. Abraham, M. C. Gaidis, G. Hu, S. Brown, Y. Zhu, R. P. Robertazzi, W. J. Gallagher, and D. C. Worledge, "Spin torque switching of 20 nm magnetic tunnel junctions with perpendicular anisotropy," *Appl. Phys. Lett.*, vol. 100, no. 13, Mar. 2012, Art. no. 132408.
[42] H. Liu, D. Bedau, D. Backes, J. A. Katine, J. Langer, and A. D. Kent, "Ultrafast switching in magnetic tunnel junction based orthogonal spin transfer devices," *Appl. Phys. Lett.*, vol. 97, no. 24, Dec. 2010, Art. no. 242510.
[43] K. Aratani, K. Ohba, T. Mizuguchi, S. Yasuda, T. Shiimoto, T. Tsushima, T. Sone, K. Endo, A. Kouchiyama, S. Sasaki, A. Maesaka, N. Yamada, and H. Narisawa, "A novel resistance memory with high scalability and nanosecond switching," in *IEDM Tech. Dig.*, Dec. 2007, pp. 783–786.
[44] Y.-Y. Lin, F.-M. Lee, Y.-C. Chen, W.-C. Chien, C.-W. Yeh, K.-Y. Hsieh, and C.-Y. Lu, "A novel Tite buffered cu-GeSbTe/SiO_2 electrochemical resistive memory (ReRAM)," in *Proc. Symp. VLSI Technol.*, Jun. 2010, pp. 91–92.
[45] E. Vianello *et al.*, "Sb-doped GeS_2 as performance and reliability booster in conductive bridge RAM," in *IEDM Tech. Dig.*, Dec. 2012, pp. 5–31.
[46] L. Zhao, Z. Jiang, H.-Y. Chen, J. Sohn, K. Okabe, B. Magyari-Kope, H.-S. P. Wong, and Y. Nishi, "Ultrathin (~2 nm) HfO_x as the fundamental resistive switching element: Thickness scaling limit, stack engineering and 3D integration," in *IEDM Tech. Dig.*, Dec. 2014, p. 6.

[47] D. C. Sekar, B. Bateman, U. Raghuram, S. Bowyer, Y. Bai, M. Calarrudo, P. Swab, J. Wu, S. Nguyen, N. Mishra, R. Meyer, M. Kellam, B. Haukness, C. Chevallier, H. Wu, H. Qian, F. Kreupl, and G. Bronner, "Technology and circuit optimization of resistive RAM for low-power, reproducible operation," in *IEDM Tech. Dig.*, Dec. 2014, pp. 3–28.

[48] L. Goux, A. Fantini, A. Redolfi, C. Y. Chen, F. F. Shi, R. Degraeve, Y. Y. Chen, T. Witters, G. Groeseneken, and M. Jurczak, "Role of the Ta scavenger electrode in the excellent switching control and reliability of a scalable low-current operated TiN Ta_2O_5 Ta RRAM device," in *Symp. VLSI Technol. (VLSI-Technol.), Dig. Tech. Papers*, Jun. 2014, pp. 1–2.

[49] Y. Matsui, K. Kurotsuchi, O. Tonomura, T. Morikawa, M. Kinoshita, Y. Fujisaki, N. Matsuzaki, S. Hanzawa, M. Terao, N. Takaura, H. Moriya, T. Iwasaki, M. Moniwa, and T. Koga, "Ta_2O_5 interfacial layer between GST and W plug enabling low power operation of phase change memories," in *IEDM Tech. Dig.*, Dec. 2006, pp. 1–4.

[50] I. S. Kim, S. L. Cho, D. H. Im, E. H. Cho, D. H. Kim, G. H. Oh, D. H. Ahn, S. O. Park, S. W. Nam, J. T. Moon, and C. H. Chung, "High performance PRAM cell scalable to sub-20 nm technology with below $4F^2$ cell size, extendable to DRAM applications," in *Proc. Symp. VLSI Technol.*, Jun. 2010, pp. 203–204.

[51] F. Xiong, M.-H. Bae, Y. Dai, A. D. Liao, A. Behnam, E. A. Carrion, S. Hong, D. Ielmini, and E. Pop, "Self-aligned nanotube–nanowire phase change memory," *Nano Lett.*, vol. 13, no. 2, pp. 464–469, 2013.

[52] C. Sun, Z. Song, A. Rath, M. Street, W. Echtenkamp, J. Feng, C. Binek, D. Morgan, and P. Voyles, "Local dielectric breakdown path along c-axis planar boundaries in Cr_2O_3 thin films," *Adv. Mater. Interface*, vol. 4, no. 20, Oct. 2017, Art. no. 1700172.

[53] S. Mu and K. D. Belashchenko, "Influence of strain and chemical substitution on the magnetic anisotropy of antiferromagnetic Cr_2O_3: An *ab-initio* study," *Phys. Rev. Mater.*, vol. 3, no. 3, Mar. 2019, Art. no. 034405.

[54] J. O. Artman, J. C. Murphy, and S. Foner, "Magnetic anisotropy in antiferromagnetic corundum-type sesquioxides," *Phys. Rev.*, vol. 138, no. 3A, pp. A912–A917, May 1965.

[55] F. W. Hehl, Y. N. Obukhov, J.-P. Rivera, and H. Schmid, "Relativistic nature of a magnetoelectric modulus of Cr_2O_3 crystals: A four-dimensional pseudoscalar and its measurement," *Phys. Rev. A, Gen. Phys.*, vol. 77, no. 2, Feb. 2008, Art. no. 022106.

[56] S. Foner, "High-field antiferromagnetic resonance in Cr_2O_3," *Phys. Rev.*, vol. 130, no. 1, pp. 183–197, Apr. 1963.

[57] X. Dong, C. Xu, Y. Xie, and N. P. Jouppi, "NVSim: A circuit-level performance, energy, and area model for emerging nonvolatile memory," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 31, no. 7, pp. 994–1007, Jun. 2012.

[58] J. J. Yang, D. B. Strukov, and D. R. Stewart, "Memristive devices for computing," *Nature Nanotechnol.*, vol. 8, no. 1, pp. 13–24, Jan. 2013.

[59] *NAND Flash 101: An Introduction to NAND Flash and How to Design it in to Your Next Product*. Accessed: Jul. 1, 2019. [Online]. Available: https://user.eng.umd.edu/~blj/CS-590.26/micron-tn2919.pdf

[60] *Comparing Technologies: MRAM vs. FRAM*. Accessed: Jul. 1, 2019. [Online]. Available: https://www.everspin.com/file/227/download

[61] T.-C. Chang, K.-C. Chang, T.-M. Tsai, T.-J. Chu, and S. M. Sze, "Resistance random access memory," *Mater. Today*, vol. 19, no. 5, pp. 254–264, Jun. 2016.

[62] A. D. Kent and D. C. Worledge, "A new spin on magnetic memories," *Nature Nanotechnol.*, vol. 10, no. 3, pp. 187–191, Mar. 2015.

[63] N. Kikuchi, S. Okamoto, and O. Kitakami, "Anomalous Hall effect measurement on nanostructure with magnetic pulse fields," *Mater. Trans.*, vol. 57, no. 6, pp. 789–795, 2016.

[64] Y.-W. Lee, H. Lim, Y. Lee, and S. Kang, "Robust secure shield architecture for detection and protection against invasive attacks," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, early access, Sep. 30, 2019, doi: 10.1109/TCAD.2019.2944580.

[65] M. Weiner, S. Manich, R. Rodriguez-Montanes, and G. Sigl, "The low area probing detector as a countermeasure against invasive attacks," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 26, no. 2, pp. 392–403, Feb. 2018.

[66] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 1999, pp. 388–397.

[67] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, Berlin, Germany: Springer, 2004, pp. 16–29.

[68] S. Ament, N. Rangarajan, A. Parthasarathy, and S. Rakheja, "Solving the stochastic Landau-Lifshitz-Gilbert-Slonczewski equation for monodomain nanomagnets: A survey and analysis of numerical techniques," 2016, *arXiv:1607.04596*. [Online]. Available: http://arxiv.org/abs/1607.04596

[69] J. Sinova, T. Jungwirth, and O. Gomonay, "Antiferromagnetic spintronics," *Phys. Status Solidi (RRL)-Rapid Res. Lett.*, vol. 11, no. 4, Apr. 2017, Art. no. 1770322.

[70] S. Shi, A. L. Wysocki, and K. D. Belashchenko, "Magnetism of chromia from first-principles calculations," *Phys. Rev. B, Condens. Matter*, vol. 79, no. 10, Mar. 2009, Art. no. 104404.

[71] M. Street, W. Echtenkamp, T. Komesu, S. Cao, P. A. Dowben, and C. Binek, "Increasing the Néel temperature of magnetoelectric chromia for voltage-controlled spintronics," *Appl. Phys. Lett.*, vol. 104, no. 22, Jun. 2014, Art. no. 222402.

[72] P. A. Dowben, C. Binek, K. Zhang, L. Wang, W.-N. Mei, J. P. Bird, U. Singisetti, X. Hong, K. L. Wang, and D. Nikonov, "Towards a strong spin–orbit coupling magnetoelectric transistor," *IEEE J. Explor. Solid-State Comput. Devices Circuits*, vol. 4, no. 1, pp. 1–9, Jun. 2018.

[73] S. Patnaik, N. Rangarajan, J. Knechtel, O. Sinanoglu, and S. Rakheja, "Advancing hardware security using polymorphic and stochastic spin-Hall effect devices," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Mar. 2018, pp. 97–102.

[74] S. Patnaik, N. Rangarajan, J. Knechtel, O. Sinanoglu, and S. Rakheja, "Spin-orbit torque devices for hardware security: From deterministic to probabilistic regime," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, early access, May 20, 2019, doi: 10.1109/TCAD.2019.2917856.

[75] K. Yogendra, M.-C. Chen, X. Fong, and K. Roy, "Domain wall motion-based low power hybrid spin-CMOS 5-bit flash analog data converter," in *Proc. 16th Int. Symp. Qual. Electron. Design*, Mar. 2015, pp. 604–609.

[76] A. Chintaluri, H. Naeimi, S. Natarajan, and A. Raychowdhury, "Analysis of defects and variations in embedded spin transfer torque (STT) MRAM arrays," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 6, no. 3, pp. 319–329, Sep. 2016.

[77] S. Swami and K. Mohanram, "Reliable nonvolatile memories: Techniques and measures," *IEEE Des. Test. IEEE Des. Test. Comput.*, vol. 34, no. 3, pp. 31–41, Jun. 2017.

[78] M. K. Qureshi, "Pay-As-You-go: Low-overhead hard-error correction for phase change memories," in *Proc. 44th Annu. IEEE/ACM Int. Symp. Microarchitecture (MICRO)*, Dec. 2011, pp. 318–328.

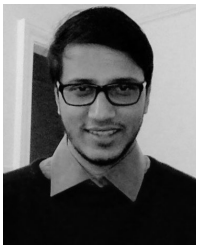
[79] R. Azevedo, J. D. Davis, K. Strauss, P. Gopalan, M. Manasse, and S. Yekhanin, "Zombie memory: Extending memory lifetime by reviving dead blocks," in *Proc. 40th Annu. Int. Symp. Comput. Archit.*, Jun. 2013, pp. 452–463.

[80] S. Chhabra, B. Rogers, Y. Solihin, and M. Prvulovic, "Making secure processors OS- and performance-friendly," *ACM Trans. Archit. Code Optim.*, vol. 5, no. 4, pp. 1–35, Mar. 2009.

[81] M. N. I. Khan, S. Bhasin, A. Yuan, A. Chattopadhyay, and S. Ghosh, "Side-channel attack on STTRAM based cache for cryptographic application," in *Proc. IEEE Int. Conf. Comput. Design (ICCD)*, Nov. 2017, pp. 33–40.

[82] J. Ferrigno and M. Hlaváč, "When AES blinks: Introducing optical side channel," *IET Inf. Secur.*, vol. 2, no. 3, pp. 94–98, 2008.

[83] A. Schlösser, D. Nedospasov, J. Krämer, S. Orlic, and J.-P. Seifert, "Simple photonic emission analysis of AES," *J. Cryptograph. Eng.*, vol. 1, no. 3, pp. 3–15, 2013.



NIKHIL RANGARAJAN (Member, IEEE) received the M.S. and Ph.D. degrees in electrical engineering from New York University, NY, USA. He is currently a Postdoctoral Associate with the Division of Engineering, New York University Abu Dhabi, United Arab Emirates. His research interests include spintronics, nanoelectronics, device physics, and hardware security.

SATWIK PATNAIK (Graduate Student Member, IEEE) received the B.E. degree in electronics and telecommunications from the University of Pune, India, and the M.Tech. degree in computer science and engineering with a specialization in VLSI design from the Indian Institute of Information Technology and Management, Gwalior, India. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, Tandon School of Engineering, New York University, Brooklyn, NY, USA. He is also a Global Ph.D. Fellow with New York University at Abu Dhabi, United Arab Emirates. His current research interests include hardware security, trust and reliability issues for CMOS, and emerging devices with a particular focus on low-power VLSI design. He is a Student Member of ACM. He received the Bronze Medal in the Graduate category at the ACM/SIGDA Student Research Competition (SRC) held at ICCAD 2018 and the Best Paper Award at the Applied Research Competition (ARC) held in conjunction with the Cyber Security Awareness Week (CSAW) in 2017.

JOHANN KNECHTEL (Member, IEEE) received the M.Sc. (Dipl.-Ing.) degree in information systems engineering and the Ph.D. (Dr.-Ing.) degree in computer engineering *(summa cum laude)* from TU Dresden, Germany, in 2010 and 2014, respectively, the Ph.D. degree with the DFG Graduate School on ''Nano- and Biotechnologies for Packaging of Electronic Systems,'' TU Dresden, in 2014. In 2010, he was a Visiting Research Student with the Department of Electrical Engineering and Computer Science, University of Michigan, USA. In 2012, he was a Research Assistant with the Department of Computer Science and Engineering, The Chinese University of Hong Kong. From 2015 to 2016, he was a Postdoctoral Researcher with the Masdar Institute of Science and Technology, Abu Dhabi. He is currently a Research Scientist with New York University Abu Dhabi, Abu Dhabi, United Arab Emirates. His research interests include VLSI physical design automation, with particular focus on emerging technologies and hardware security.

OZGUR SINANOGLU (Senior Member, IEEE) received the B.S. degree in electrical and electronics engineering and in computer engineering from Boğaziçi University, Turkey, in 1999, and the M.S. and Ph.D. degrees in computer science and engineering from the University of California at San Diego, in 2001 and 2004, respectively.

He has industry experience at TI, IBM, and Qualcomm. He has been with NYU Abu Dhabi since 2010. He is currently a Professor of electrical and computer engineering with New York University Abu Dhabi. He is the Director of the Design-for-Excellence Lab, NYU Abu Dhabi. His recent research in hardware security and trust is being funded by the U.S. National Science Foundation, the U.S. Department of Defense, Semiconductor Research Corporation, Intel Corp, and Mubadala Technology. He has given more than a dozen tutorials on hardware security and trust in leading CAD and test conferences, such as DAC, DATE, ITC, VTS, ETS, ICCD, ISQED, and so on. His research interests include design-for-test, design-for-security, and design-for-trust for VLSI circuits, where he has more than 180 conference and journal articles, and 20 issued and pending U.S. Patents.

Dr. Sinanoglu received the IBM PhD Fellowship Award twice during his Ph.D. He was also a recipient of the best paper awards at the IEEE VLSI Test Symposium 2011 and ACM Conference on Computer and Communication Security 2013. is serving as a Track/Topic Chair or a Technical Program Committee Member for about 15 conferences and as a (Guest) Associate Editor for IEEE TIFS, IEEE TCAD, ACM JETC, IEEE TETC, Elsevier MEJ, JETTA, and IET CDT journals.

SHALOO RAKHEJA (Member, IEEE) received the M.S. and Ph.D. degrees in electrical and computer engineering from the Georgia Institute of Technology, Atlanta, GA, USA. She was an Assistant Professor of electrical and computer engineering with New York University, Brooklyn, NY, USA. She was a Postdoctoral Research Associate with Microsystems Technology Laboratories, Massachusetts Institute of Technology, Cambridge, USA. She is currently an Assistant Professor of electrical and computer engineering with the Holonyak Micro and Nanotechnology Laboratory, University of Illinois at Urbana–Champaign, Urbana, IL, USA, where she works on nanoelectronic devices and circuits.