Self-Correcting STTRAM under Magnetic Field Attacks

Jae-Won Jang[1], Jongsun Park[2], Swaroop Ghosh[1], Swarup Bhunia[3]
[1] Computer Science and Engineering, University of South Florida, Tampa, Florida, USA
[2] School of Electrical Engineering Korea University, Seongbuk-Gu, Seoul, South Korea
[3] Case Western Reserve University, Cleveland, Ohio, USA
jjang3@mail.usf.edu, jongsun@korea.ac.kr, sghosh@cse.usf.edu, skb21@case.edu

***Abstract*—Spin-Transfer Torque Random Access Memory (STTRAM) is a possible candidate for universal memory due to its high-speed, low-power, non-volatility, and low cost. Although attractive, STTRAM is susceptible to contactless tampering through malicious exposure to magnetic field with the intention to steal or modify the bitcell content. In this paper, for the first time to our knowledge, we analyze the impact of magnetic attacks on STTRAM using micro-magnetic simulations. Next, we propose a novel array-based sensor to detect the polarity and magnitude of such attacks and then propose two design techniques to mitigate the attack, namely, array sleep with encoding and variable strength Error Correction Code (ECC). Simulation results indicate that the proposed sensor can reliably detect an attack and provide sufficient compensation window (few ns to ~100us) to enable proactive protection measures. Finally, we shows that variable-strength ECC can adapt correction capability to tolerate failures with various strength of an attack.**

***Keywords*—**STTRAM, Magnetic field attack, Contactless tampering, Variable ECC, Replica, On-chip tamper mitigation

I. INTRODUCTION

Spin-Transfer Torque RAM (STTRAM) [1] is a promising memory technology due to high-speed, low-power, non-volatility, and low cost. The commercialization of Magnetic RAM (MRAM) has fueled the development of STTRAM further as the potential future memory technology. STTRAM is an energy-efficient modification of MRAM [2], where the switching of the magnetization is accomplished through current induced spin-transfer torque. STTRAM offers fast and low-power switching via use of spin-polarized current. Due to density closer to DRAM, speed closer to SRAM, high endurance and superb retention time, STTRAM is widely considered to be a suitable candidate for Universal Memory [7-8]. Fig. 1 shows the STTRAM cell schematic, where the Magnetic Tunnel Junction (MTJ) is used as the storage element. The MTJ contains a free layer and a pinned magnetic layer. The resistance of the MTJ stack is high (low) if free layer magnetic orientation is anti-parallel (parallel) compared to the fixed layer. The configuration of the MTJ can be changed from parallel to anti-parallel (or vice versa) by injecting current from source-line to bitline (or vice versa). The spin-torque transfer phenomena for reversal of magnetization in free layer reduce the write power compared to conventional MRAM.

DAC '15, June 07 - 11, 2015, San Francisco, CA, USA

978-1-4503-3520-1/15/06…$15.00
http://dx.doi.org/10.1145/2744769.2744909

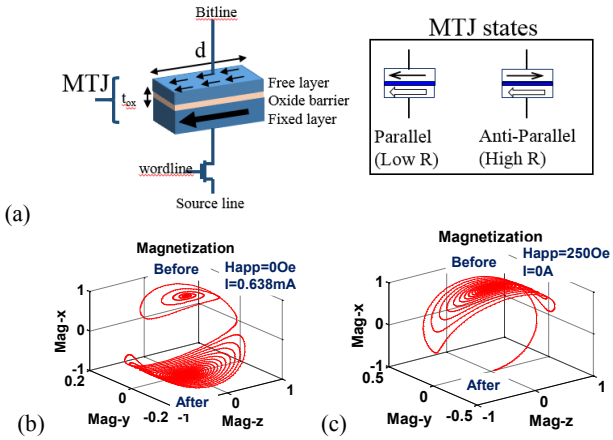


Fig. 1(a) Schematic of STTRAM bitcell showing MTJ; (b) flipping of MTJ free layer due to STT (Happ=0Oe, I=0.638mA); and, (c) due to external magnetic field (Happ=260Oe, I=0). The plots are obtained by solving LLG from (1).

Although STTRAM is a promising memory technology, it brings in an important security concern. It is susceptible to contactless tampering efforts, e.g. by subjecting it to strong external magnetic field, an adversary can corrupt stored contents. The fixed layer of STTRAM is robust. However, the free layer could be toggled through both spin polarized current as well as magnetic field. The free layer is susceptible to both the magnitude and polarity of external magnetic field it is subjected to. The motivation of tampering for an adversary is to corrupt the data or steal information. This could prevent STTRAMs application to a wide range of mobile devices. Fig. 1 (b)-(c) shows that the MTJ free layer could flip its polarity either using current or with 250Oe magnetic field. The magnetic field produced by a common horseshoe magnet is ~126Oe [3] which is sufficient to flip the weak bits in presence of process variations and thermal noise. Note that although we take STTRAM as motivational case study, other forms of magnetic memories such as MRAM, Domain Wall Memory (DWM) and Ferroelectric RAM (FRAM) [4] is also expected to experience similar issue, and hence vulnerable to tampering attacks. The ease of tampering the data using low-cost commercially available magnets underscores the need of quantifying the impact of magnetic attack and exploring effective, low-overhead protection mechanisms [5].

In this paper, for the first time, to the best of our knowledge, we demonstrate the impact of magnetic field based tampering in STTRAM. We propose an on-chip sensor based on replica of a memory in order to accurately detect the magnitude and polarity of an attack. This information is employed for on-chip compensation to nullify the magnetic attack. We propose two techniques - array

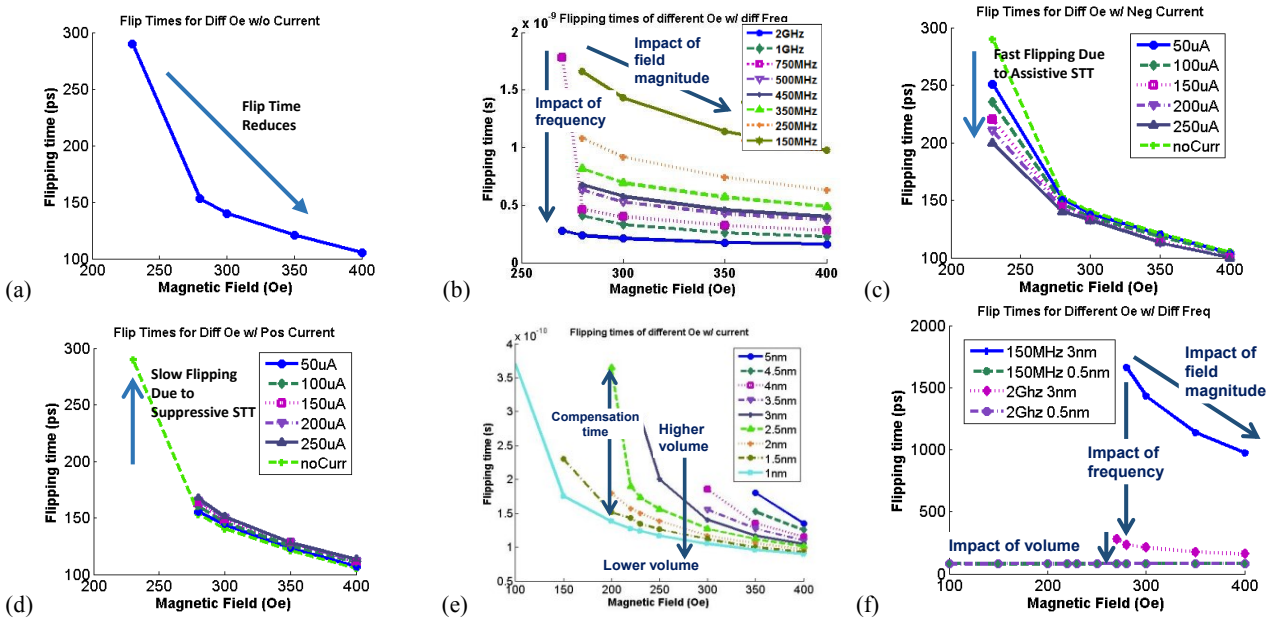


Fig. 2. Impact of magnetic field on the stability of free-layer: The flipping time reduces with (a) DC magnetic field; and (b) AC magnetic field. Impact of functional operation on the flip time in presence of (c) assistive current; and (d) suppressing current. Impact of MTJ volume on the flip time in presence of (e) DC; and (f) AC magnetic field.

retention and adaptive variable strength Error Correcting Code (ECC) to protect the bits in STTRAM against magnetic attacks.

In summary, we make following major contributions in this paper:

- We investigate the impact of magnetic attack on an STTRAM array. We consider both DC and AC attack modes.
- We propose an array-based sensor to detect the magnitude and polarity of an attack. The sensor array is deliberately designed to be more sensitive to attack (than the memory core) by reducing the free-layer volume and weak write.
- We monitor the bit error rate (BER) of sensor array and take proactive steps to mitigate the attack. Our investigation reveals that retention mode is robust to attack. Therefore, we propose array retention during attack.
- Finally, we present a dynamic error-rate dependent variable-strength ECC to mitigate the bit failures due to attacks.

The rest of the paper is organized as follows. In Section II, we present the magnetic attack model and quantify the impact on memory error rate. The magnetic field sensor design is introduced in Section III. The on-chip compensation and correction methodology are proposed in Section IV and the simulation results are presented in Section V. Conclusions are drawn in Section VI.

II. MAGNETIC ATTACK ON STTRAM

In this section, we present the attack model, quantify the impact on memory stability, and describe the impact of process variation.

A. Background on MTJ

The magnetization orientation of the pinned layer is fixed using an anti-ferromagnetic coupling and it cannot be changed using nominal current or external magnetic field. Contrary to this, the free layer could be toggled by passing current or by applying magnetic field. The magnetization dynamics of the MTJ free layer is governed by LLG equation [6].

$$\frac{\partial \vec{m}}{\partial t} = \underbrace{-\gamma \vec{m} \times \overrightarrow{H_{eff}} - \alpha\gamma \vec{m} \times \vec{m} \times \overrightarrow{H_{eff}}}_{\text{Field term}} + \underbrace{\frac{I_s \hbar G(\psi)}{2e} \vec{m} \times (\vec{m} \times \overrightarrow{e_p})}_{\text{STT term}} \quad (1)$$

TABLE-I. 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

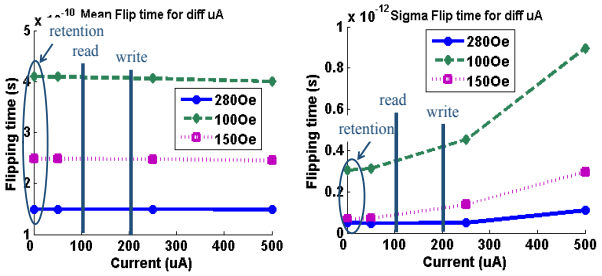
where $\vec{m}$ is unit vectors representing local magnetic moment, I_s is spin current, $G(\psi)$ is the transmission co-efficient, $\hbar$ is reduced planck's constant, α is Gilbert damping parameter and $\overrightarrow{e_p}$ is the unit vector along fixed layer magnetization. The effective field is represented by $\overrightarrow{H_{eff}} = \overrightarrow{H_a} + \overrightarrow{H_k} + \overrightarrow{H_d} + \overrightarrow{H_{ex}}$, where H_a is applied field, H_k is anisotropy field, H_d is demagnetization field and H_{ex} is exchange field.

In STTRAM the writing of MTJ is done using STT term (for low power consumption) and external field H_a is kept 0. However, H_a can also be used to toggle the magnetization in absence of charge current (field term, eq (1)). Note that magnetic field-based toggling is the foundation of MRAM. 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.

B. Attack Model

The attacks on STTRAM could be launched either through static (DC) magnetic field or alternating (AC) magnetic field. The DC attack is less detrimental as it can only create unipolar failures. For example, a magnetic field will cause failures only for the bits whose free layer orientation is opposite to the applied field. However, the AC field could cause more damage as it will affect both storage polarities. Due to ease of AC field generation using a low-cost electromagnet this type of attack is highly likely.

The attack could be launched either during ideal (retention) mode or functional mode (read/write). Note that read current is unipolar



(a) (b)

Fig. 3. Impact of process variations on flip time during retention and functional mode (a) mean; and, (b) sigma.

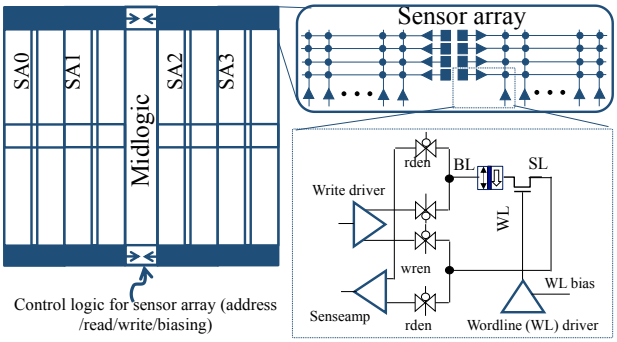


Fig. 4. Embedded attack sensor in memory array. The details of sensor array with peripheral circuits is shown in inset. Control logic is shared among the subarrays and contains the logic to generate address, read, write and data and analyze the response.

irrespective to the storage polarity whereas write current polarity is data dependent. The impact of attack during functional mode (especially read) could be more detrimental than retention due to two factors: (a) presence of disturb current; and, (b) higher frequency of reads compared to writes. Both storage polarity will be affected under AC attack. During write operation, the AC field will either assist if the current polarity matches with the magnetic field or suppresses the attack if the current polarity is opposite to applied field. In all of the above scenarios the attack could either manifest as hard failure (i.e., flipping of bitcell content) or soft failure (i.e., delay in write or degraded sense margin). The soft failures could be mitigated by slowing down the read/write operation but the hard failures need to be avoided or corrected through error correction.

The frequency of the magnetic field is important in the context of failures in functional mode. If the AC field frequency is faster than the write time then it can affect writing both data polarities. Similarly it can also affect both storage polarities during read operation. If the frequency of AC field is slow then the impact will be less harmful.

C. *Attack Analysis*

We use publicly available micro-magnetic simulator OOMMF [9-10] to analyze the impact of DC and AC magnetic field tampering on the integrity of STTRAM. The MTJ parameters used for sim is shown in Table 1. It can be noted from Fig. 2(a) that the MTJ polarity could be flipped in retention mode. The flip time reduces with increasing strength of magnetic field. The impact of AC field is plotted in Fig. 2(b). For this simulation we have used a sinusoidal field and varied the frequency from 150MHz to 2GHz. It can be observed that higher frequency AC field can cause more damage even with smaller amplitude than lower frequency AC field and higher amplitude.

The comparison of MTJ stability between retention and functional mode is considered in Fig. 2(c)-(d). For the analysis we have assumed different magnitudes of read/write currents and polarities for both DC and AC fields. For DC field, it can be observed that the bits can 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). Similar observation also holds true for AC 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. For this simulation we have swept the MTJ thickness from 3nm to 0.5nm. Fig. 2(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. 2(f)) indicate that higher volume can protect against attack of lower frequency. High frequency attack can cause failure regardless of MTJ volume.

D. *Impact of Process Variation*

For the large caches, process variation in MTJ and access transistor can modulate the failure characteristics in presence of tampering.

Process variation is also crucial for sensor design and detection of strength of attack. In this work we have considered the variations in access transistor and MTJ volume. The access transistor variation is lumped in threshold voltage variation. The (mean, sigma) of V_{TH} variation is assumed to be (0, 50mV). The volume variation (mean, sigma) is assumed to be (0, 5%). The LLG model [11-12] is ported to verilogA (after calibration with OOMMF) and used for fast circuit simulation. The impact of variations on failures during retention as well as functional mode are evaluated. A total of 5000 Monte Carlo points are simulated for analysis.

Fig. 3(a)-(b) shows the mean and sigma of flip time for different strength of DC magnetic field. For functional mode we have considered 50uA, 250uA and 500uA initial assistive current using a voltage source. It can be noted that mean flip time reduces in functional mode 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 regardless of variability*. This feature can be exploited for mitigating the impact of attack (Section IV). The functional mode (read/write) amplifies the impact of variability and results in random bit errors.

III. TAMPER DETECTION SENSOR

In this section, we describe the design of a novel tamper detection sensor for magnetic memory based on a memory replica (similar to critical path replicas that monitor path delay variations in a chip).

A. *Sensor Design*

The key objective of the proposed 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: (a) the intensity of the attack; and (b) the polarity of the attack, both of which can be useful in auto-protecting a memory subsystem against data corruption.

We use a small replica of the STTRAM array 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. 4). 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

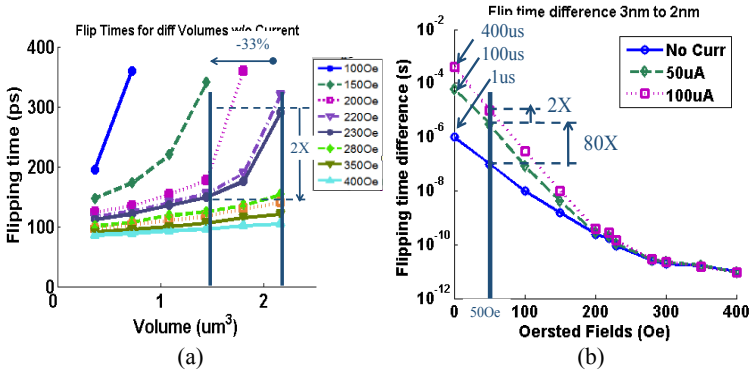


Fig. 5. Sensitivity free layer volume on flip time: (a) 33% reduction in volume reduces flip time by 2X; (b) effectives of volume scaling and weak write on early detection of attack. Reduction of 33% volume can detect 50Oe attack ~100ns before actual array fails. Weak write of 50uA can provide 80X more time. An additional 50uA can provide 2X extra time.

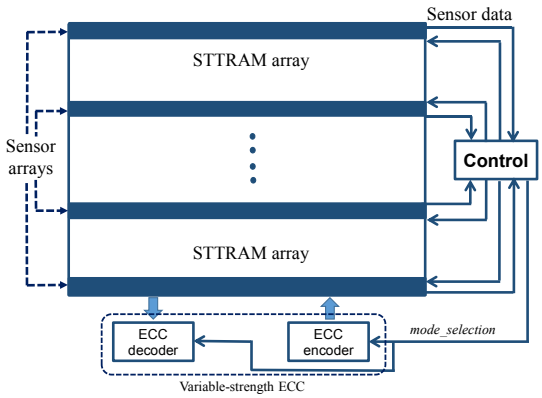


Fig. 6. Overall system protection approach that includes an STTRAM array with embedded sensors, attack mitigation, and variable-strength ECC.

to higher intensity. The proposed sensors have following salient features to quantify the intensity and polarity of attack:

(a) 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.

(b) Distribution of sensors: These different flavors of sensors can be distributed in the cache to collect the spatial responses.

(c) Weak writing/stress: This technique lowers the activation energy of MTJ so that it fails early. 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. 4). The column multiplexers are kept ON to enable weak writing of all columns.

(d) 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.

(e) 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).

(f) 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 re-initialize 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 100ns before the real bits and test takes 25ns then the time available to enable mitigation techniques (which is compensation window) is 75ns.

(g) 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. 4).

(h) 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 (a) interleaved with normal sensors (sensor-n); and, (b) turned on periodically.

B. Simulation Results

Fig. 5 (a)-(b) shows the sensitivity of free layer volume with respect to the flip time of DC attack. 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. We compute the flip time difference between functional MTJs and sensor MTJs and plot them in Fig. 5(b). For lower fields we extrapolate the flip time difference. The sensor MTJ uses 33% lower volume (sensor-n). The results indicate that a 50Oe attack could be detected ~100ns before the real bits is corrupted. For weak attacks (<10Oe) the sensor can detect it ~1us in advance. By adding 50uA of current (for sensor-w) the sensitivity could be improved by ~80X at the cost of extra power overhead. An additional 50uA can improve the sensitivity by an additional 2X.

From 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 4 local columns and 128 rows per sensor array, the weak writing could cause 25mW power (at 1V) 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 is less than 1% since they are embedded in the transition region of the arrays.

IV. On-Chip Compensation

The sensor proposed in the previous section is used to sense polarity and intensity of attack and trigger two types of compensation mechanisms namely, array sleep and variable strength ECC.

A. Compensation Methodology

Fig. 6 shows the top level schematic of the proposed sensing and compensation methodology. The attack could be DC as well as AC and the magnitude could vary temporally and spatially. To capture the spatial variation we distribute the sensors 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.

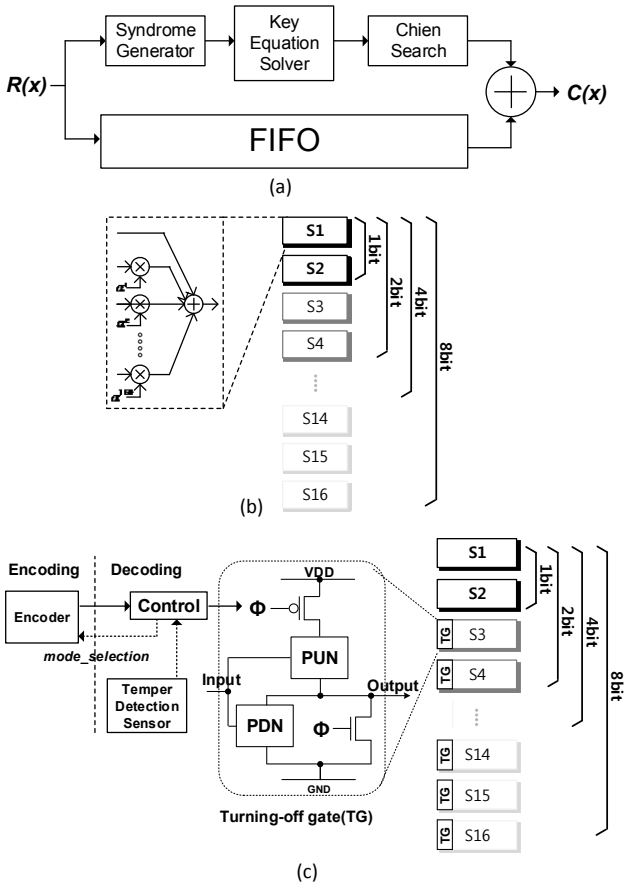


Fig. 7. Variable-strength ECC architecture (a) BCH decoding process, (b) An example of scalable syndrome generator, (c) Dynamic reconfiguration scheme applied to syndrome generator using turning-off gate [12]. The turn-off signal Φ is generated from control module.

B. Array Sleep

From Section IID it is evident 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 (Section V). 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.

C. Variable-Strength ECC

In addition to on-chip electromagnet, variable-strength ECC is used to correct failures in STTRAM. The proposed ECC can provide variable error correction capability to STTRAM array based on the strength of magnetic field attack. The variable-strength ECC 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, we used Bose-Chaudhuri-Hocquenghem (BCH) cyclic code with 128 bit data-length. The variable-strength ECC offers four different error correction capabilities (1bit/ 2bit/ 4bit/ 8bit), 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 it can be working with simplest ECC (1 bit correction). As the magnitude of attack is becoming intense, which can be measured at detection sensor, the control unit in Fig.7 (a) can adapt ECC to provide stronger error corrections (2bit/ 4bit/ 8bit corrections). When smaller error correction options are selected, the unused modules in the ECC can be easily turned off to save computation energy.

TABLE -II. Hardware implementation results of VC ECC

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

(a) Variable-strength ECC encoder: 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 (1bit / 2bit / 4bit/ 8bit). 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.

(b) Variable-strength ECC decoder: The VC-ECC decoder is basically similar to 8 bit 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 bits.

First, the syndrome generator of the VC-ECC decoder is similar to that of 8bit correction BCH. As shown in Fig. 7 (b), since the syndrome generator for 1bit, 2bit or 4 bit correction BCH can be expressed as a subset of syndrome generator for 8 bit correction BCH [13], 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 bit, 2 bit or 4 bit correction BCH, respectively. Key equation solver (KES) and Chien search modules can be designed scalable like Syndrome generator, and the unused module can be simply turned off using the turning-off scheme. The turning-off scheme applied to Syndrome generator is illustrated in Fig. 7(c). Simple pull-up and pull-down transistors with correct dimensions is being used based on whether 1-bit, 2-bit, 4-bit or 8-bit 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 [14].

The proposed variable-strength ECC decoder is implemented using 65-nm standard-cell CMOS library, and Table II shows the implementation results. Separate 1-bit (Hamming), 2-bit, 4-bit and 8-bit correction BCH decoders are also implemented for comparison. The power consumptions of various BCH decoders are measured at 100MHz, 1.2V with spice-level simulations using 1000 input data. As the error correction capability increases, the area requirement is understandably larger. The additional area for turning-off gates and control logic are accounted for in the results presented in Table II. The area overhead of the proposed variable ECC is not significant compared to 8-bit correction BCH decoder.

(c) Dynamic adaptation scheme: The proposed variable-strength ECC has four choices of error correction capabilities, and the correction mode can be controlled using 2 bit *mode selection* signal as shown in Fig. 6 and Fig. 7 (c). This *mode selection* signal is generated from control logic, and the information is updated at

TABLE-III. Bit error rates (BERs) VC ECC is applied to STTRAM cells attacked with various strengths of magnetic fields.

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	$5.7*10^{-6}$

runtime on a regular basis by monitoring the magnetic attack strength at temper 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-bit *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 [15]. The two bit overhead for the *mode selection* storage is negligible (< 0.3% area overhead) considering a typical cache block size (e.g. 512bits). If we cannot correct a block due to inadequate correction capability, then we can set its dirty bit and fetch it from the next level. If we're using the memory as last level of memory, then even higher protection is needed. In the proposed ECC, another way of checking the occurrence of STTRAM failures by ECC itself is to monitor the outputs of syndrome generator since any non-zero syndrome indicates memory failure occurrence. This syndrome monitoring scheme can be used to check the frequency of STTRAM failures in the functional mode.

V. Results And Discussions

TABLE-III 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 100μA means that 76.9Oe is combined with 100μA current to model active operation mode. According to the results, when the magnetic attack strength of 76.8Oe 100μA is used, STTRAM cells show raw BER of $3*10^{-3}$. In this case, ECC with 4 bit corrections (t=4) can be selected to correct STTRAM bit failures. When the attack strength is as large as 76.9Oe 500μA, the STTRAM raw BER is too large ($9.7*10^{-1}$) that the failures cannot be corrected even with 8 bit correctable ECC. However, the proposed 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 we detect bit failures which are too many to correct by the current ECC, then we can invalidate the corresponding cache blocks, thus preventing use of wrong data.

The information in Table III 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 100μA, the ECC correction capability (t) of the proposed variable-strength ECC can be decided as t=2. Then, the memory data is read out, re-encoded to match the correction capability of ECC to the level of external field and written back to memory before it goes to array sleep.

VI. Conclusions

We demonstrated the possibility of a contactless tampering using common magnet or electromagnet on STTRAM for the first time. Our analysis indicated that an adversary can achieve significant success in destroying the data by creating a strong external magnetic field, which can be accomplished even with low-cost publicly accessible magnets. We quantified the impact of such attack using a widely used micro-magnetic simulation framework from NIST. Next, we have presented a novel sensor based on memory replica that can detect memory corruption due to such an attack ahead of time along with the intensity and polarity of a magnetic field attack. Finally, we have presented two low-overhead effective design solutions to mitigate the attack, namely, (1) array sleep; and (2) variable strength Error Correction Code (ECC) that can dynamically adapt its correction capability. Both protection approaches rely on the sensor's output – e.g., the variable ECC dynamically adapts error protection based on sensed intensity of the filed. These solutions together can provide high level of protection against such attacks. They solutions can also be effective to counter effect of naturally-present (non-malicious) magnetic field induced failures in specific applications (e.g. geo-thermal exploration). Future work will include further optimization of sensor design; analysis of other forms of contactless tampering attacks (e.g. with an electromagnetic field); and investigation of similar attacks in other forms of memory (e.g. resistive or phase change memory).

VII. Acknowledgement

This paper is based on work supported by Semiconductor Research Corporation (#2442.001), National Research Foundation of Korea (#2012R1A2A2A01012471), IC Design Education Center (IDEC), and NSF Awards #1054744, #1245756, and #1441757.

VIII. References

[1] Driskill-Smith, A. Latest advances and future prospects of STT-RAM. In Non-Volatile Memories Workshop. 2010.
[2] J.-G. Zhu, "Magnetoresistive Random Access Memory: Path to Competiveness and Scalability", Proceedings of the IEEE, 2008.
[3] http://en.wikipedia.org/wiki/Magnet.
[4] Kryder, Mark H et al. "After hard drives—What comes next?." Magnetics, IEEE Transactions on 45, no. 10 (2009): 3406-3413.
[5] SGMI Research Themes & Subjects. Online: http://www.samsung.com/global/business/semiconductor/html/news-events/file/SGMI_Request_for_Proposal.pdf
[6] Zhang, Jianwei et al. Identification of transverse spin currents in noncollinear magnetic structures. Physical review letters 93, no. 25 (2004): 256602.
[7] Kultursay, Emre, Mahmut Kandemir, Anand Sivasubramaniam, and Onur Mutlu. "Evaluating STT-RAM as an energy-efficient main memory alternative." In Performance Analysis of Systems and Software (ISPASS), 2013 IEEE International Symposium on, pp. 256-267. IEEE, 2013.
[8] E. Chen et al. Advances and Future Prospects of Spin-Transfer Torque Random Access Memory. Magnetics, IEEE Transactions on, 46(6), June 2010.
[9] Donahue, Michael Joseph et al. OOMMF User's guide. US Department of Commerce, Technology Administration, National Institute of Standards and Technology, 1999.
[10] Nikonov, D. Online Lecture, Topic: "Course on Beyond CMOS Computing." June. 06, 2013. https://nanohub.org/resources/18347
[11] Srinivasan, Srikant. "All spin logic: Modeling multi-magnet networks interacting via spin currents." (2012).
[12] Behin-Aein, Behtash et al, "Proposal for an all- spin logic device with built-in memory", Nature nanotechnology 5, no. 4 (2010): 266-270.
[13] J. Park et al. "Dynamic Bit-width Adaptation in DCT: An Approach for Trade off Image Quality and Computation Energy", *IEEE Trans. on VLSI*, vol. 18, no. 5, pp. 787-793, May 2010.
[14] S. Lin et al, *Error Control Coding*, 2nd ed. Prentice Hall, 2004.
[15] S. Paul et al, "Reliability-Driven ECC Allocation for Multiple Bit Error Resilience in Processor Cache", *IEEE Trans. Comput*. 2011.