Correlation Power Analysis Attack against STT-MRAM Based Cyptosystems

Abhishek Chakraborty, Ankit Mondal, and Ankur Srivastava
Department of Electrical and Computer Engineering,
University of Maryland, College Park, USA
Email: $\{abhi1990, amondal2, ankurs\}@umd.edu$

***Abstract*—Emerging technologies such as Spin-transfer torque magnetic random-access memory (STT-MRAM) are considered potential candidates for implementing low-power, high density storage systems. The vulnerability of such nonvolatile memory (NVM) based cryptosystems to standard side-channel attacks must be thoroughly assessed before deploying them in practice. In this paper, we outline a generic Correlation Power Analysis (CPA) attack strategy against STT-MRAM based cryptographic designs using a new power model. In our proposed attack methodology, an adversary exploits the power consumption patterns during the write operation of an STT-MRAM based cryptographic implementation to successfully retrieve the *secret* key. In order to validate our proposed attack technique, we mounted a CPA attack on MICKEY-128 2.0 stream cipher design consisting of STT-MRAM cells with Magnetic Tunnel Junctions (MTJs) as storage elements. The results of the experiments show that the STT-MRAM based implementation of the cipher circuit is susceptible to standard differential power analysis attack strategy provided a suitable hypothetical power model (such as the one proposed in this paper) is selected. In addition, we also investigated the effectiveness of state-of-the-art side-channel attack countermeasures for MRAMs and found that our proposed scheme is able to break such protected implementations as well.**

***Index Terms*—Correlation power analysis attack, Spin-transfer torque magnetic RAM, MICKEY-128 2.0 stream cipher**

I. Introduction

Spin-transfer torque magnetic random-access memory (STT-MRAM) is an emerging nonvolatile memory alternative that has high density, low power requirements, and compatibility with existing DRAM and SRAM designs[1].It exhibits superior endurance and lower access latencies compared to other existing flash memory technologies. In fact, STT-MRAM outperforms conventional magnetoresistive random-access memory in terms of low power requirement as well as scalability [2]. Field Programmable Gate Arrays (FPGAs) using STT based low power Look-Up-Tables(LUTs) have been proposed which utilize the programmability of Magnetic Tunnel Junctions (MTJs) [3], [4]. However, the security of such STT based implementations must be thoroughly verified before they are used in commercial applications since such designs may be vulnerable to *non-invasive* reverse engineering, such as side-channel analysis, to obtain detailed design trademarks.

Side-channel attacks exploit the unintentional information leakage from the real-life implementation of a cipher algorithm to retrieve the *secret* key. Power analysis attack is a form of passive side-channel analysis technique where the adversary monitors the power consumption of a cipher design without tampering any operation of the underlying algorithm [5]. In [6], the authors have proposed the use of hybrid STT-CMOS design flow in which a selected number of CMOS gates from a synthesized gate-level netlist are replaced with reconfigurable STT based LUT counterparts to enhance system security against reverse engineering attacks. It has also been claimed that such STT based implementations are more resistant to power based side-channel analysis techniques compared to CMOS based designs due to low sensitivity of power consumption to input changes.

However, recent works such as [7], [8] have exposed the susceptibility of STT based implementations to side-channel attack methods using standard side-channel leakage models. In [7], the authors have also proposed several countermeasures to mitigate simple power analysis attacks against MRAM based implementations. In this paper, we propose a Correlation Power Analysis (CPA) attack scheme by applying a new hypothetical power model to estimate the power consumption of MTJ based cipher designs after vertical *alignment* of the collected power traces. CPA is a kind of differential power analysis approach, where the adversary monitors the functional dependency of a cryptosystem's power leakage and the data being processed during targeted time window. We demonstrate that our proposed power analysis technique defeats the state-of-the-art side-channel attack countermeasures [7].

In order to validate our proposed attack methodology, we considered an implementation of eSTREAM hardware portfolio finalist MICKEY-128 2.0 stream cipher[9]. We first mounted a CPA attack against a standard hardware design of the cipher in which the registers were considered to be MRAM based memory array and observed that the adversary can successfully retrieve the *secret* key using a low number of power side-channel traces. We also demonstrated the vulnerability of the cipher design to CPA attack even in presence of state-of-the art countermeasures for MTJ based designs, as proposed in [7]. The technique presented in this paper outlines a generic methodology which can be utilized to mount such differential power analysis attacks on MRAM based implementations of other cipher algorithms such as block cipher, public key cryptosystems, etc.

The remainder of the paper is organized as follows: In section II, we provide some preliminary concepts related to the working principle and power consumption characteristics of an MTJ device. Section III describes in detail our proposed hypothetical power model to estimate the *post alignment* power consumption of an MTJ based hardware implementation. In section IV, we present the CPA attack strategy against an MRAM based design of MICKEY-128 2.0 stream cipher using our proposed hypothetical intermediate power

value model. Section V reports the experimental results of our proposed attack scheme for both standard and protected MRAM based implementations of the stream cipher MICKEY-128 2.0. Finally, section VI concludes the paper.

II. Preliminaries

In this section, we first describe in detail the principles of Magnetic Tunnel Junctions (MTJs). We then present the circuit of MRAMs (MTJ-based memory cells) and characterize the dependence of their write power consumption on the data.

A. MTJ Basics

MTJ is the most popular spintronic device being considered for NVM technologies [1]. Apart from non-volatility, its high integration density, scalability and CMOS compatibility make it a suitable candidate for replacing CMOS in future memory devices. It consists primarily of 3 layers - two ferromagnetic layers made of CoFeB, and an oxide (typically MgO) layer sandwiched between them acting like a tunnel barrier. The magnetic orientation of one the magnetic layers (called the Pinned or Fixed Layer, PL) is fixed in a direction, whereas that of the other layer (called the Free Layer, FL) can be toggled. This gives rise to two distinct states, depending on whether the orientations are Parallel (P) or Anti-Parallel (AP) to each other. The AP state exhibits a higher resistance than the P state which are characterized by the Tunnel Magnetoresistance Ratio $TMR = (R_{AP} - R_P)/R_P$ It is this difference which allows us to store information - the P state represents logic 0 whereas the AP state logic 1. Depending on the magnetic anisotropy, MTJs are categorized into two - In-plane (IMTJ) and Perpendicular(PMTJ). Fig. 1 shows both the configurations.

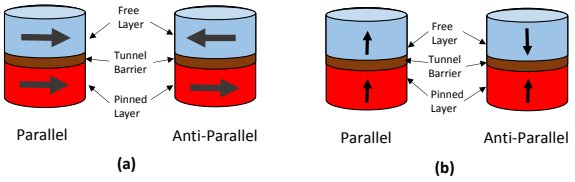


Fig. 1: Schematic of MTJ showing parallel and anti-parallel states with (a) In-Plane and (b) Perpendicular anisotropy. Arrows show direction of magnetic orientation.

The state of the MTJ can be switched by passing spin-polarized current in the appropriate direction [10]. If the magnitude and duration of the current are sufficient, it reverses the magnetization of the Free layer through a transfer of angular momentum as illustrated in Fig. 2.

When the switching time of MTJs is in the range of a few ns (which we call the precessional mode of switching [11] [12]),it is inversely related to the current density as follows:

$$t_{sw} \propto (J - J_{c0})^{-1} \tag{1}$$

where J_{c0} is the critical switching current density and is different for the two switching directions. Specifically $J_{c0} \propto \eta^{-1}$ where $\eta = (P/2)/(1 + P^2 cos\theta)$ is the spin transfer efficiency [13], P is the spin polarization factor of the FL and θ is the angle between the magnetic orientations of the FL and PL (0 for P state and π for AP state). This indicates higher switching current requirements of the P→AP transition for the same switching time and vice versa. The PMTJ has a lower critical switching current density and better scalability prospects as compared to its in-plane counterpart and so, in this paper, we consider PMTJ for implementing MRAM cell arrays.

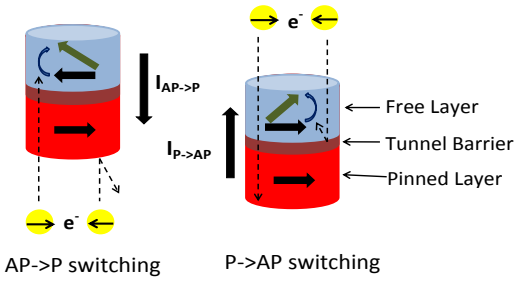


Fig. 2: MTJ switching through STT mechanism. Notice how unpolarized current becomes polarized.

B. STT-MRAM Cell

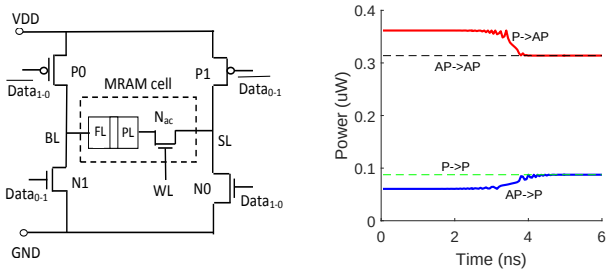
An STT-MRAM bit cell consists of an MTJ and an access transistor, which is typically an NMOS, joined in series. This is called the 1-Transistor 1-Junction (1T1J) configuration. They are connected to the Bit Line (BL) at one end and to the Source Line (SL) at the other. The gate of the transistor is connected to the Word Line (WL) which is made high whenever it is required to select this MTJ for writing or reading purposes. When the MTJ is to be written, a voltage difference of sufficient magnitude is created between the BL and the SL, with the polarity depending on the data to be written. For reading the data stored, a small voltage bias is used to sense the current flowing through the MTJ and compare it to a reference current, in order to determine its resistance state.

The BL and SL are connected to the write driver which contains the control circuit (comprising PMOS and NMOS transistors) for deciding the direction of current flow. Fig. 3a shows the MRAM cell along with the write driver. Note, however, that while writing 1, the gate-source voltage of N_{ac} depends on the voltage on the MTJ as $V_{GS} = V_{WL} - V_{MTJ} - V_{BL}$ [1]. This increases the threshold voltage of N_{ac} due to substrate effect ($V_{SB} > 0$), reducing the current flow and introducing further asymmetry. Proper sizing of write driver transistors is necessary to ensure that the current through the MTJ is as desired for both switching directions.

C. MTJ switching characteristics

There are 2 modes of writing to the MTJ.

- Constant Voltage - The voltage supply for switching remains constant throughout the duration of the write pulse. The current through the write path changes as the MTJ switches (due to change in its resistance).
- Constant Current - The current through the write path is maintained at a constant value with the help of current mirrors. The voltage drop across the MTJ changes as its switches.



(a) (b)

Fig. 3: (a) The MRAM cell consisting of the MTJ and the access transistor N_{ac}. The 4 transistors external to it are part of the write driver. (b) Power levels and variation for P $\rightarrow$ AP and AP $\rightarrow$ P switching. Note that power remains constant in the absence of any switching as shown by the dashed lines

To obtain MTJ switching characteristics, we use a physics-based HSPICE model [14]. The variation of current, and hence power, with time for both switching directions with a constant voltage supply is illustrated in Fig 3b. The power changes exactly when the FL orientation switching takes place. As discussed in the previous subsection, the asymmetric nature of the MTJ switching requires us to supply higher current or have longer pulse width for changing the state from 0 to 1. In this work, we operate in the constant voltage mode; and to obtain same switching time, we ensure larger current for writing 1 through suitable transistor sizing.

III. Power Analysis of MTJ device

The power consumption profiles of MTJ devices are significantly different from that of standard CMOS cells. In case of CMOS based implementation of a flip-flop, which is widely used to store state information, we can approximate the power consumption due to different state transitions as follows:

$$P(0,0) \approx P(1,1) << P(0,1) \approx P(1,0) \tag{2}$$

where, $P(i,j)$ denotes the transition power from state i to state j, and $i,j \in \{0,1\}$. The dynamic power consumption of a CMOS cell will depend on the nature of switching as shown below:

$$P_{CMOS}^{dynamic} \in \{P_{CMOS}(0,1), P_{CMOS}(1,0)\} \tag{3}$$

However, such an approximation is not valid for an MTJ device as evident from the discussion in section II-C. Unlike a CMOS device, the power consumption $P_{MTJ}(i,i)$, $i \in \{0,1\}$, of an MTJ based MRAM cell in absence of any transition is also of significant magnitude. We can consider the power consumption P_{MTJ} of an MTJ device to be depending on the nature of state transition as follows:

$$P_{MTJ} \in \{P_{MTJ}(0,0), P_{MTJ}(1,1), P_{MTJ}(0,1), P_{MTJ}(1,0)\} \tag{4}$$

It is to be noted that the switching power $P_{MTJ}(i,j)$ of an MTJ for transition from state i to state j ($i \neq j$, and $i,j \in \{0,1\}$) is not only of different magnitudes but also results in alteration of power profiles in opposite directions (as shown in figure 3b). In other words, an MTJ device switching from AP to P results in an increase in power consumption, while the transition from P to AP results in a decrement in the power consumption. In the next subsection, we discuss the impact of these variations of power consumption patterns on power analysis attacks.

A. Hypothetical Power Model

In a standard power analysis attack framework, an adversary estimates the power leakages associated with a targeted *intermediate value* using a suitable hypothetical power model. The success of a power analysis attack against a cryptosystem largely depends on the accuracy of such estimations of the associated leakages. One of the most popular models that is used to estimate the power consumption of a CMOS based implementation is the Hamming distance (HD) power model [5]. In order to mount a Differential Power Analysis (DPA) attack on a CMOS based cryptographic design, an adversary uses equation 3 to model the power consumption being proportional to HD of a targeted *intermediate value* , i.e., $P_{total}^{CMOS} \propto HD$.

However, such proportionality will not be accurate enough to model the power consumption of an MTJ device as its power profile varies depending on the nature of the underlying transitions. Therefore, the power consumption of a design consisting of n MTJ storage elements can be modeled as follows:

$$P_{total} \propto t_{00}P(0,0)+t_{11}P(1,1)+t_{10}P(1,0)+t_{01}P(0,1) \tag{5}$$

where, t_{ij} denote the number of transitions from state i to j, $i,j \in \{0,1\}$. It is to be noted that $n = t_{00}+t_{11}+t_{10}+t_{01}$. In context of DPA attack, an adversary usually performs vertical alignment of the power traces collected from the targeted device by subtracting the DC bias from every time sample instants of the trace. In this paper, we compute the aforementioned DC bias by averaging a small number of power values at the beginning of a targeted clock cycle of the cipher design where there is no transition of power consumption due to MTJ write operation. If we *vertically align* the power traces collected during the operation of an MTJ based crypto implementation, the factors P(0,0) and P(1,1) will not contribute any significant information to the DPA adversary as there is no variation in power profile due to such transitions. Therefore, *post-alignment* of the collected power traces, the total power consumption of the implementation can be approximated as follows:

$$P_{total}^{align} \propto t_{10}P(1,0) + t_{01}P(0,1) \tag{6}$$

In a standard DPA attack framework [5], after collection of power traces during a targeted *attack window*, statistical analysis is performed to exploit the relationship between the power traces and the key-dependent hypotheses of *intermediate value*. Even though an adversary is able to obtain the values of t_{01} and t_{10} for the targeted *intermediate value* corresponding to different key guesses, she will not have any notion of the power consumption magnitudes of a single MTJ for such transitions. This is due to the consideration that DPA is a *non-profiling* side-channel attack technique [5]. Therefore, in order to successfully mount a power analysis attack against such an MTJ based implementation, the adversary first needs

to setup a hypothetical power model to estimate the associated leakages. In this paper, we exploit the nature of power profile alteration due to switching of an MTJ device from AP to P and vice-versa for estimating the overall power leakage of the cryptosystem.

From figure 3b, we observe that when an MTJ switches from AP to P state, there is an increase in power consumption. Thus, for an MTJ based MRAM cell array, the increase in power consumption (after *alignment* of the traces) is proportional to the number of AP to P switching, i.e., $\Delta P^{align}_{AP\rightarrow P} \propto t_{10}$. On the other hand when the state of an MTJ switches from P to AP , there is a decrease in power consumption and thus, the decrement in power consumption of an MTJ based MRAM cell array is proportional to the number of such transitions, i.e., $\Delta P^{align}_{P\rightarrow AP} \propto -t_{01}$ Therefore, the overall variation of power consumption of an MRAM cell array can be modeled as follows:

$$\Delta P^{align}_{total} \propto at_{10} - bt_{01} \tag{7}$$

where, a and b are device dependent parameters that correspond to the magnitude of power profile alteration due to AP→P and P→AP transitions respectively. We assume that a DPA adversary cannot *profile* such device characteristics and hence, uses $\Delta P^{align}_{total} = t_{10} - t_{01}$ to estimate power consumption in a targeted *attack window* for MTJ based implementation of a cipher design.

IV. CPA attack on MTJ based designs

In order to mount a Correlation Power Analysis (CPA) attack on a cryptographic implementation, an adversary exploits the correlation between the collected power traces of the design and the cipher algorithm's operands/operations being performed during a targeted time frame. The ultimate objective of the adversary is to successfully retrieve the *secret* key based on the results of statistical analysis on the captured power traces using the notion of underlying operations being carried out in the targeted time window. One of the most widely used techniques to compute the linear relationship between the estimated power consumption values and the actual power traces is to calculate the Pearson's correlation coefficient metric.

In this paper, we consider an implementation of stream cipher MICKEY-128 2.0 to demonstrate the vulnerability of MTJ based designs to side-channel analysis attacks. Similar steps can be followed to break MTJ based implementations of other cryptographic algorithms like block ciphers, public key ciphers, etc.

A. MICKEY-128 2.0 stream cipher

The MICKEY-128 2.0 stream cipher was selected as a hardware oriented finalist of the eSTREAM project [9]. The hardware design of the cipher [15] is shown in figure 4. It was primarily proposed for lightweight cryptographic implementations and its design consists of two 160 bit registers: a Linear Feedback Shift Register (R) and a Nonlinear Feedback Shift Register (S). The input parameters of MICKEY-128 2.0 are: 128 bit *secret* key and n bit initialization vector ($n \in \{0, 128\}$, we considered $n = 128$). The details of the cipher algorithm, in accordance with which the states of R and S are updated along with generation of the *keystream*, are outlined in [9]. In this paper the register stages are considered to be made up of STT-MRAM cells with MTJs as storage units.

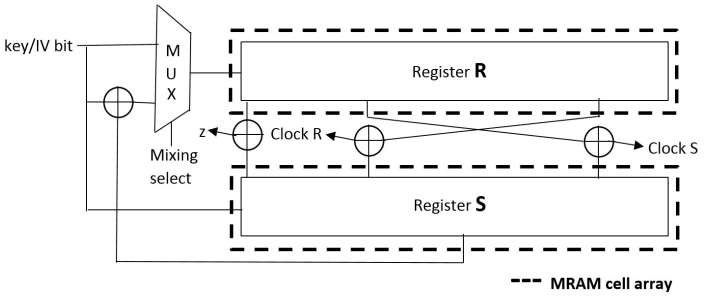


Fig. 4: Hardware realization of MICKEY-128 2.0 [15]

B. Overview of CPA attack

We broadly follow the CPA attack framework as discussed in [15] to break an MRAM based implementation of MICKEY-128 2.0 stream cipher. However, we consider a different hypothetical power model (as outlined in section III-A) to estimate the associated side-channel leakages. The major steps of the CPA attack can be summarized as follows:

- First, the adversary usually identifies a key-dependent *intermediate value* of the targeted cryptographic algorithm [5]. In the context of the MICKEY-128 2.0 stream cipher, we considered all the *stages* of both the registers, R and S, as the *intermediate value* during the entire key loading phase of the cipher.
- The second step involves collection of power traces during the execution of the cipher. Unlike block ciphers, power analyses of stream ciphers usually require to capture the leakage associated with several consecutive clock cycles or rounds of operations rather than targeting a particular round. In a standard CPA framework against a stream cipher such as MICKEY-128 2.0, an adversary resynchronizes its hardware implementation with several different Initialization Vectors (IVs) for a fixed *secret* key to obtain a sufficiently large number of power traces.
- Finally, she estimates the leakages using a suitable hypothetical power model, followed by employment of statistical measures to compare the actual power consumption values with the prior estimated leakage values for a targeted key loading round of MICKEY-128 2.0 stream cipher. In the ensuing attack strategy, we considered the hypothetical power model described in section III-A to estimate the power consumption and used Pearson's correlation coefficient metric for statistical analysis.

Once a key bit was determined from the correlation profile, the subsequent key bit was targeted using the same procedure after selection of a new *window* of sample points for the corresponding key bit. We can repeat this attack strategy for different key bit loading rounds to recover entire 128 bits of the *secret* key in an iterative manner.

V. Experimental Results

In this section, we first outline in detail the technique that we adopted to generate simulated power traces for an MRAM

based design. Then, we report the experimental results of CPA attack against an MTJ based implementation of the MICKEY-128 2.0 stream cipher using our proposed hypothetical power model to estimate the associated leakages of the targeted *intermediate value*. In addition, we also report the experimental results of CPA attack against a protected implementation of the cipher.

A. Trace generation

In our experiments we used a device physics based MTJ simulator [14] written in HSPICE to evaluate the power consumption of a single MRAM cell. The MTJ specifications used for the purpose are summarized in Table I. We assumed a clock period of 5 ns as both P $\rightarrow$ AP and AP $\rightarrow$ P transitions complete within that time frame. Subsequently, we generated the power traces for the entire MICKEY-128 2.0 implementation by superimposing the power consumption values due to transitions of all MTJs in the design (considering both register R and S).

Parameter	Value
MTJ dimensions	35nm X 35nm X 1.4nm
Spin Polarization Factor (P)	0.85
Saturation Magnetization	1030 emu/cc
Damping constant	0.014
RA product	5 $\Omega\mu m^2$
Temperature	300 K

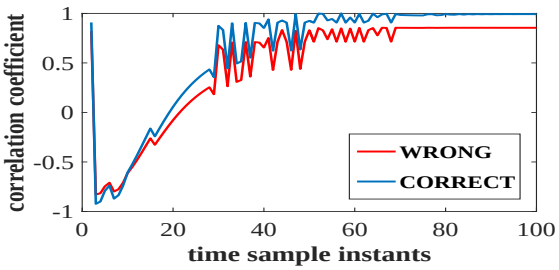
TABLE I: MTJ device parameters used for simulation

B. CPA attack results

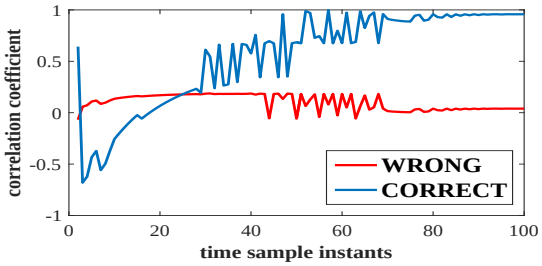
In this section, we present the results of Correlation Power Analysis (CPA) attack on simulated traces for the MTJ based implementation of MICKEY-128 2.0 stream cipher. We considered the hypothetical power model as described in section III-A to estimate the power consumption of the overall circuit after *alignment* of the power traces and subsequently performed power analysis. The power traces of the implementation were simulated by *resynchronizing* the cipher operation multiple times with randomly generated 128 bit Initialization Vectors for a fixed 128 bit key value.

The results of the CPA attack against a standard design of MICKEY-128 2.0 are shown in figure 5. The plots correspond to a targeted window of time sample points for a randomly selected key bit loading round of the cipher. The sub-figures 5a and 5b show the nature of variations of Pearson's correlation coefficient between the simulated power consumption at different sample instants and the corresponding estimated power values (using our proposed hypothetical power model) for different key bit guesses across the *attack window*.

It can be observed from the nature of the correlation plots that the *correct* key bit guess (shown in blue) can be easily distinguished from the *wrong* key bit guess (shown in red) as the number of traces considered for analysis is increased. In the current implementation, around 50 power traces were sufficient to retrieve the correct key bit. Once the targeted key bit is successfully determined, the adversary selects a new *window* of power samples to attack the subsequent key bit. This process is repeated in an iterative manner till all/sufficient number of key bits are retrieved. We repeated the experiment targeting various such key loading rounds of MICKEY-128 2.0 and observed similar trends in correlation profiles separating



(a) Number of traces: 10



(b) Number of traces: 50

Fig. 5: *Time sample instants* vs. *Correlation coefficient* for correct (shown in blue) and wrong (shown in red) key bit guesses for **standard** design of MICKEY-128 2.0

the correct key bit guesses from the wrong ones. In figure 6, we present the result of CPA attack targeting 5 consecutive key bit loading rounds of the cipher to show such trends. Similar standard power analysis techniques can be mounted on MTJ based implementations of other cipher algorithms, provided a suitable hypothetical power model, as the one proposed in this paper, is chosen by the adversary.

1) CPA on protected design: In this subsection, we present the results of the CPA attack against a state-of-the-art protected implementation of cipher design using the hypothetical *intermediate value* selection (as outlined in section III-A) to estimate the power consumption.

In [7], the authors have outlined a countermeasure to secure an MTJ based design against side-channel attacks by using random updates of additional registers in the circuit to mask the power consumption due to actual registers in the cipher module. Though, such a countermeasure can safeguard a cipher against Simple Power Analysis (SPA) attacks, such cryptosystems will still be susceptible to CPA attacks. In figure 7, we present the results of CPA attack on a MTJ based protected implementation of MICKEY-128 2.0 stream cipher which incorporates such 160 additional registers (updated randomly in each round of operation).

It can be observed from the nature of the correlation profiles, that the *correct* key bit guess (shown in blue) can be clearly distinguished from the *wrong* key bit guess (shown in red) as the number of traces considered for analysis is increased to 100. Therefore, even the inclusion of a large number of random register updates (50% MTJ area overhead), the cipher design is still vulnerable to CPA attack using a reasonably low number of side-channel traces using our proposed power model. Moreover, if a constant current source is used for MRAM write operation, then also the implementation will be

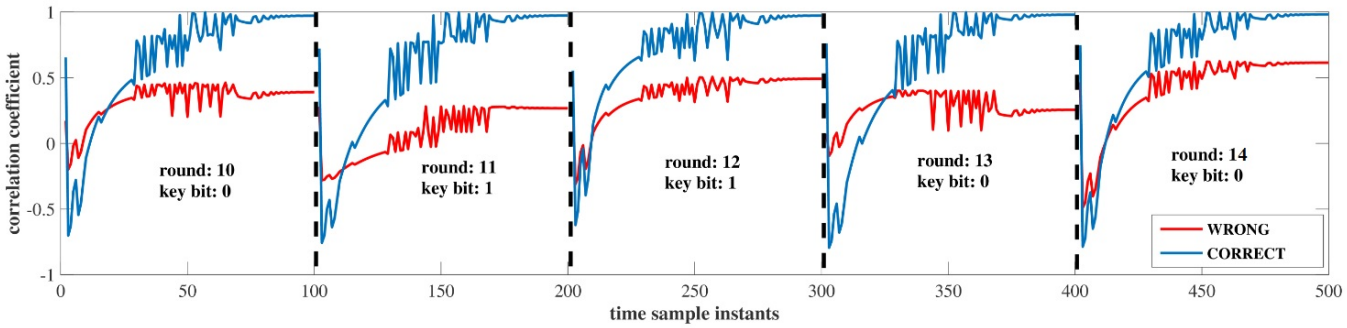
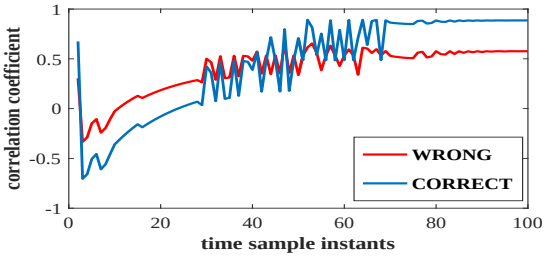
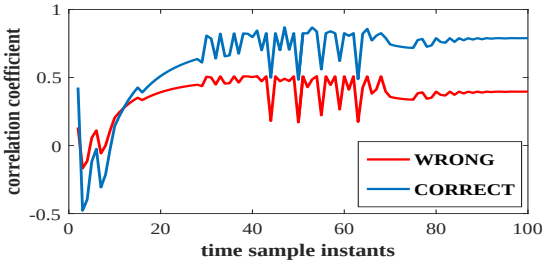


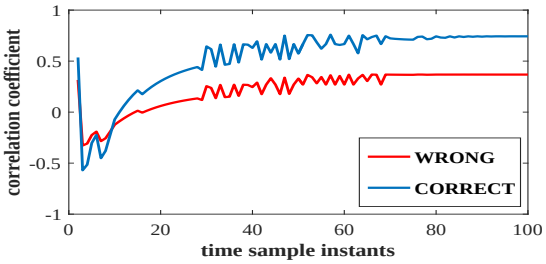
Fig. 6: *Time sample instants* vs. *Correlation coefficient* for correct (shown in blue) and wrong (shown in red) key bit guesses across 5 consecutive attack rounds with key bit sequence 01101 (Number of traces considered: 50)



(a) Number of traces: 10



(b) Number of traces: 50



(c) Number of traces: 100

Fig. 7: *Time sample instants* vs. *Correlation coefficient* for correct (shown in blue) and wrong (shown in red) key bit guesses for **protected** design of MICKEY-128 2.0

susceptible to our proposed CPA attack strategy as the power consumed by the MRAM cell will still vary depending upon the voltage drops across MTJ devices.

VI. Conclusion

In this paper we demonstrated the susceptibility of MTJ based implementations of cryptosystems to differential side-channel attacks where the adversary uses multiple number of traces to retrieve the *secret* key. We proposed a new hypothetical power model that considers the difference of transitions $1 \rightarrow 0$ and $0 \rightarrow 1$ to estimate the *post-alignment* power consumption of an MTJ based cipher design. We considered the stream cipher MICKEY-128 2.0 to validate our proposed scheme and performed Correlation Power Analysis (CPA) attack on both standard and state-of-the-art protected implementation of the cipher. The results of the experiments confirm that both the aforementioned design configurations of the cipher are vulnerable to differential side-channel attack. The hypothetical power model proposed in this paper can be utilized to break MTJ based implementations of other cipher algorithms as well.

References

[1] D. Apalkov et al., "Spin-transfer torque magnetic random access memory (stt-mram)," *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, vol. 9, no. 2, p. 13, 2013.

[2] R. A. Lukaszew, *Handbook of Nanomagnetism: Applications and Tools*. CRC Press, 2015.

[3] D. Suzuki et al., "Fabrication of a nonvolatile lookup-table circuit chip using magneto/ semiconductor-hybrid structure for an immediate-power-up field programmable gate array," in *2009 Symposium on VLSI Circuits*. IEEE, 2009, pp. 80–81.

[4] H. Mahmoodi et al., "Resistive computation: A critique," *IEEE Computer Architecture Letters*, vol. 13, pp. 89–92, 2014.

[5] T. P. Stefen Mangard, Elisabeth Oswald, *Power Analysis Attacks revealing the secrets of Smart Cards*. Springer, 2007.

[6] T. Winograd et al., "Hybrid stt-cmos designs for reverse-engineering prevention," in *Proceedings of the 53rd Annual Design Automation Conference*. ACM, 2016, p. 88.

[7] A. Iyengar, S. Ghosh, N. Rathi, and H. Naeimi, "Side channel attacks on sttram and low-overhead countermeasures," in *Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2016 IEEE International Symposium on*, 2016, pp. 141–146.

[8] J.-W. Jang et al., "Self-correcting sttram under magnetic field attacks," in *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*. IEEE, 2015, pp. 1–6.

[9] S. Babbage and M. Dodd, "The stream cipher mickey-128 2.0. estream, ecrypt stream cipher project, 2006," *Avaiable at: http://www. ecrypt. eu. org/*, 2013.

[10] J. Kim et al., "Spin-based computing: device concepts, current status, and a case study on a high-performance microprocessor," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 106–130, 2015.

[11] Z. Li and S. Zhang, "Magnetization dynamics with a spin-transfer torque," *Physical Review B*, 2003.

[12] Y. Huai, "Spin-transfer torque mram (stt-mram): Challenges and prospects," *AAPPS Bulletin*, vol. 18, pp. 33–40, 2008.

[13] Y. Zhang et al., "Asymmetry of mtj switching and its implication to stt-ram designs," in *Proceedings of the Conference on Design, Automation and Test in Europe*, ser. DATE '12, 2012, pp. 1313–1318.

[14] J. Kim et al., "A technology-agnostic mtj spice model with user-defined dimensions for stt-mram scalability studies," in *Custom Integrated Circuits Conference (CICC), 2015 IEEE*, 2015, pp. 1–4.

[15] A. Chakraborty and D. Mukhopadhyay, "A practical template attack on mickey-128 2.0 using pso generated ivs and ls-svm," in *2016 29th International Conference on VLSI Design (VLSID)*, 2016, pp. 529–534.