International Journal of Innovation and Scientific Research
ISSN 2351-8014 Vol. 22 No. 2 Apr. 2016, pp. 356-363

http://www.ijisr.issr-journals.org/

Design of Cascaded PADDL for DPA-Resistant Secure Integrated Circuits Using Penta Magnetic Tunnel Junction

T.R. Dineshkumar[1], M. Anto Bennet[2], V. Priyanka[3], M. Priya[3], and T. Ruby[3]

[1]Assistant Professor, Department of Electronics and Communication Engineering, VEL TECH, Chennai-600062, India

[2]Professor, Department of Electronics and Communication Engineering, VEL TECH, Chennai-600062, India

[3]UG Student, Department of Electronics and Communication Engineering, VEL TECH, Chennai-600062, India

ABSTRACT: A novel design methodology is to implement a secure DPA resistant crypto secured processor such as advanced encryption standard (AES) and triple data encryption standard (DES), by secure side-channel attacks, such as differential power analysis (DPA). The methodology is suitable for integration in a common automated standard cell ASIC or FPGA design flow. Dynamic logic is obfuscates the output waveforms and the circuit operation, which reducing the effectiveness of the DPA attack for mitigating DPA attacks for applications of secure integrated circuit (IC) design. A Penta MTJ gate that provides self-referencing, simple cascading, less voltage headroom downside in pre charge sense electronic equipment and low space. These types of gate is implemented in (PADDL). Different logic gates and different writing circuitry is required, but the sensing portion is remains same. Therefore, the information is deposited in the pinned layers using series or parallel combinations of transistors as per the logic storing in the Penta MTJ. The logic gate is authenticated by simulation at the 22nm technology node using a tanner tool.

KEYWORDS: High-performance adiabatic dynamics differential logics (PADDL), Differential power Analysis (DPA) Attack, Penta MTJ, Magnetic tunnel junction, Magneto resistance, precharge sense amplifier (PCSA).

1 INTRODUCTION

Spintronics has been under extensive research because of non-volatility, endless endurance, and low power [1].The spin is hired for storing information and the charge for its processing. It has the potential to replace CMOS logic and memory [2]. In bottomless sub-micrometer, scaling of CMOS causes the leakage power to dominate over all other power components [3]. Digital signals are represented in conventional CMOS logic by the existence or nonexistence of electrical charge in terms of voltage VDD or ground. However, in spintronics, digital signals are represented by up and down spin of electron. In recent years, researchers have developed spintronic devices, such as magnetic tunnel junctions (MTJs), which operates on the principle of tunnel magnetoresistance (TMR) [4]. An MTJ is composed of two ferromagnetic layers detached by an oxide layer with the ability to improve the performance of CMOS logic circuit in terms of power dissipation, area required, and interconnection delay [5]. It can also be easily fabricated using 3-D backend integrationprocess, which is compatible with CMOS process, without any area overhead [6].

Corresponding Author: T.R. Dineshkumar

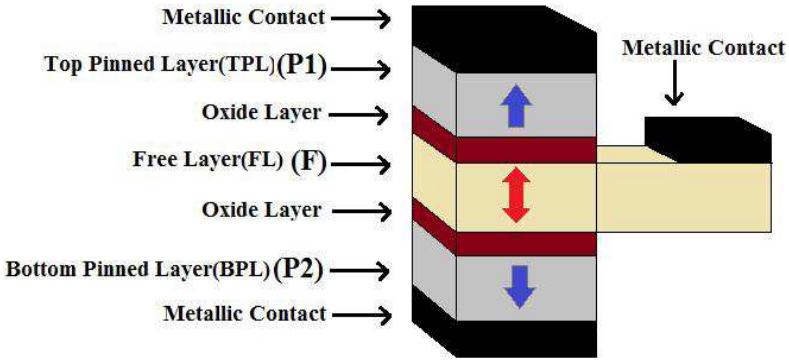

Fig.1. Structure of Penta MTJ with two pinned layers (TPL and BPL) and one free layer

MTJ has two properties such as processing and storage. Which helps to reduce the memory and interconnect delay/power[7] are needed to store the processed data back into memory. In [8] a magnetic XOR gate is containing six MTJs and the transistors. The area requirement is less nevertheless the number of MTJ increases and the writing energy also increases, which is a serious drawback of the hybrid circuit consisting of MTJ and CMOS. Friedman et al.[9] and Horowitz and Hill[10] proposed a spin diode and CMOS logic circuit respectively, which has the static power dissipation is more compared to the within power dissipation. This is due to the requirement of constant VDD supply for a node of spin-diode and the leakage-power dissipation in CMOS at the Nano scale, respectively.

SMART cards are any compact-size card that has embedded circuits. Smart cards are made up of plastic or tokens. it may provide a personal identification, authentication, data storage and application processing. They are used as credit or ATM cards , fuel cards , mobile phone SIMs, authorization cards for pay television, household utility pre-payment cards, high-security identification and access-control cards, and public transport and public phone payment cards. They are used in specific application so their size and software overhead may be minimized. In addition, smart cards are using a tamper resistant secure file system of crypto processor. They can provide a strong security authentication. In case of theft they can be programmed to preventing immediate reuse. It is more effective than cards. Due to their special importance on security to both software and hardware levels, smart card technology is moving towards multiple applications, higher interoperability, and multiple interfaces, such as TCP/IP, near-field communicators, and contactless chips.

Despite of secure software design, They still susceptible to side-channel attack, which is based on correlations of leaked secondary information and the output signal of IC. They include electromagnetic leakage, measuring[15] the amount of time required to perform private-key operations[14] and analysis of noisy power consumption[15]. In this the most effective attack is Differential Power Analysis attack(DPA)[16],where the attacker analyzes the power consumption in IC and it compares to the output of the signal. Due to the presence of entropy gain of the system provides a leaked side channel information.DPA attack is more effective, since most of the modern computing technology is based on CMOS. In this device reducing the power consumption makes the DPA attack more difficult. In this paper the design and analysis using high-performance adiabatic dynamic differential (PADDL) logic for effectiveness of DPA attack, which is a novel universal cell that perform a AND,OR,NAND,XOR,XNOR and NOR operations. The instantaneous power, average power and differential power of the PADDL cell are compared to the same metrics of conventional NAND, NOR and XNOR gates. In this paper spintronic is used instead of CMOS logic. The spin is used for storing information and charge for its processing. It has replaced to CMOS logic and memory, because leakage power is dominate the overall other power consumptions. Digital signal are represented in CMOS logic is presence and absence of electric charge in terms of voltage VDD or GND.

2 MOTIVATION AND BACKGROUND

A. DPA ATTACKS

In software systems security and hardware oriented security requires a two prong approach to smart card security. Smart card are not isolated in perfectly tamper proof location and it utilize operating system with cryptographic kernels and the memory devices are used to store. The result analysis of a chip's operation metrics are differential power consumption, radio frequencies, total execution time and magnetic field values allows attackers to gain sensitive user data.DPA attack is the use of power consumption to obtain their compromising information. In modern computing system use CMOS technology and in CMOS gate, the dynamic power consumption is proportional to its input signals[4]. Therefore,the analyze

of output power consumption allows the attacker to determination of correlation between data and key. since the CMOS gates switching is dependent on those inputs.

B. DPA PREVENTION

The primary drawbacks are addressing DPA attacks in the software level is that the power and the current variations being a analyzed by attacker occurs in the hardware level, and there is no software alogrithm,however it is effective but it can be affects the operation of a CMOS gate once it receives an input signal. Therefore, the most effective approach is to prevention of DPA attack includes security-based logic within the hardware implementation itself and to make it difficult for the attacker to ascertain the necessary information to determine their inputs. The three most important metrics are consider when designing CMOS circuits, such as power consumption, area, and operating frequency, since Ediss = C L *Vdd2 * f , where CL is the load capacitance, Vdd is the supply voltage, and f is the operating frequency.

C. PROPOSED PADDL CELL

In this section, we present method for implementation of PADDL design methodology for mitigating DPA attacks in high-performance applications. The data presented in this section was obtained using HPSICE simulations using the 22-nm predictive technology model presented [17].

The objective of PADDL is to design as a universal cell capable of dynamically performing all of the fundamental two-input logical calculations (AND, NAND, OR, NOR, XOR, and XOR) with the minimal differential power for each logical calculation. The device is both logically and physically bijective. This means that the input waveforms may be uniquely determined by reading the output waveforms, a necessity in implementation of low-power reversible and adiabatic designs.

The logical calculations of the output signals of PADDL are P = A_, P_ = A, Q = (A + B) $\oplus$ C, Q_ = (A + B) $\oplus$ C,R = AB $\oplus$ C, and R_ = AB $\oplus$ C.

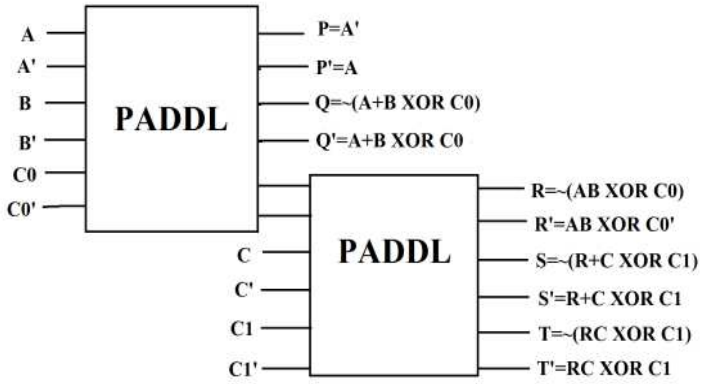

Fig.2 Cascaded PADDL cells with logic outputs shown

The arrows in the basic square diagram indicate what will occur if the signal shown is a logic 1. For example, in Fig. 2(a), if A is a logic 1, then there exists a path from C to Q, meaning that the logical values of C and Q will be equivalent. This is because the pMOS/nMOS pair will have the nMOS with 1 and the pMOS with 0, and the path will be activated. InFig. 2(b), the path from C to R will be switched OFF if A or B is 1. This is because the pMOS/nMOS pair will have the nMOS with 0 and the pMOS with 1. Therefore, to have C equal to R, then A must be 0, and B must be 0.

TABLE I.TRUTH TABLE FOR PROPOSED PADDL CELL

A	A'	B	B'	C	C'	P	P'	Q	Q'	R	R'
0	1	0	1	0	1	1	0	1	0	1	0
0	1	0	1	1	0	1	0	0	1	0	1
0	1	1	0	0	1	1	0	0	1	1	0
0	1	1	0	1	0	1	0	1	0	0	1
1	0	0	1	0	1	0	1	0	1	1	0
1	0	0	1	1	0	0	1	1	0	0	1
1	0	1	0	0	1	0	1	0	1	0	1
1	0	1	0	1	0	0	1	1	0	1	0

Control signal	P	P'	Q	Q'	R	R'
A=0	A'	A	$\overline{B \oplus C}$	$B \oplus C$	C'	C
A=1	A'	A	C'	C	$\overline{B \oplus C}$	$B \oplus C$
B=0	A'	A	$\overline{A \oplus C}$	$A \oplus C$	C'	C
B=1	A'	A	C'	C	$\overline{B \oplus C}$	$B \oplus C$
C=0	A'	A	$\overline{A+B}$	A+B	$\overline{AB}$	AB
C=1	A'	A	A+B	$\overline{A+B}$	AB	$\overline{AB}$

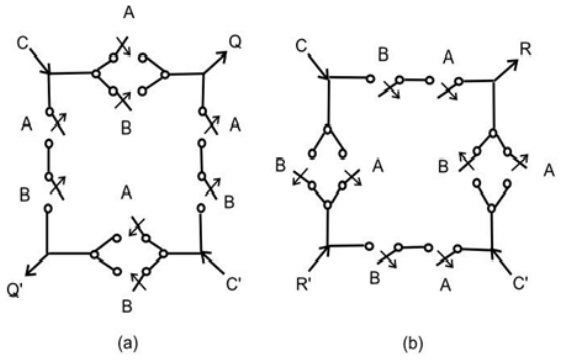

Fig. 3.Basic square circuit diagram for the proposed PADDL cell.(a) Logical calculations for the Q and Q_ outputs based on the A, B, and C inputs

The device has 32 transistors.it have their gate, drain, and source tied to an input or output signal. The pMOS transistors are biased to the minimal supply voltage, which is 0.8 V in the 22-nm model in [17], and the nMOS transistors are biased to ground. The advantage of this approach is that evaluation and discharge signals are not required, meaning that less powerrepresents the R and R_ output signals. The bottom waveform is the instantaneous power.

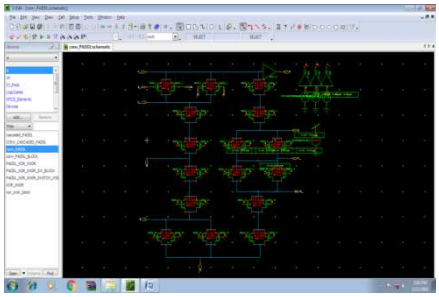

Fig 4.Conventional PADDL schematic diagram

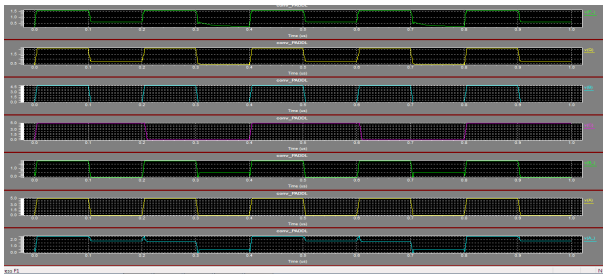

Fig 5. Simulation result for convential PADDL

3 COMPARISON TO PREVIOUS BENCHMARKS

Here, we compare our presented PADDL method with previous benchmarks in mitigation of DPA Attacks, SDMLp [18], ring- and counter-controlled delay logic (RCCDL) [19], and WDDL [20]. We reproduced those circuits in 22-nm technology using the methods presented in those papers. The average power consumption of each of these methods, as well as the conventional implementation in CMOS, is presented in Table III.The presented PADDL design is advantageous to the previous designs in average power for each of the fundamental calculations AND, NAND, OR, NOR, XOR, and XNOR. PADDL improves upon SDMLp by 76.41%, over RCCDL by 93.98%, and by 89.65% over WDDL. The implementation of SDMLp is the previously best implementation, since it uses evaluate and discharge phases. Locally, SDMLp is advantageous in terms of required transistors, since implementation of SDMLp requires 16 transistors as opposed to the 32 transistors needed in our proposed implementation. However, this advantage is erased when cascading the cells together. The hardware overhead required ensuring proper timing of evaluation and discharge stages of each cell increases exponentially as the length of the critical path of the device increases. The PADDL circuit does not require any overhead for maintaining evaluation and discharge phases, making it the better cell for larger implementations, such as DES circuits. However improving the area of the PADDL device is important. We address this issue in the next section through the use of body biasing in subthreshold operation of the adiabatic dynamic differential logic (ADDL).

In Table IV, we present the results of the average energy dissipation during the state transitions of the PADDL com-pared with the previously presented work. The frequency is 13.56 MHz, and the rise and fall times of the state transitions are 1.8436*10−8 s.

Table 2.Comparison of power

LOGIC	CMOS	WDDL	RCDDL	SDMLp	PADDL
AND	2.9182	6.9751	11.99717	3.705	0.8596
NAND	2.6382	6.4056	11.01763	3.705	0.8596
OR	2.8106	7.2350	12.4442	3.718	0.8596
NOR	3.0702	7.2350	12.18568	3.718	0.8596
XOR	3.3451	11.0587	19.02096	3.508	0.8587
XNOR	3.3451	11.0587	19.02096	3.508	0.8587
Avg	3.0212	8.3029	14.2811	3.643	0.8593
StdDev	0.2626	1.9653	3.380437	0.0961	0.0004
Transistor Required For Universal	26	42	32	16	32
Cell Area(nm^2)	505752	816983	622462	341622	532022

Eventhough PADDL has better than the other memory cells,such as ADDL,BADDL,WADDL and SDMLp.it is also has some drawbacks like more power consumption and delay because of its conventional XOR/XNOR logic so that we are adding pentaMTJ based XOR/XNOR logic for better performance

4 PENTA MTJ

1)(TPL) and 2) bottom pinned layer (BPL). The magnetizations of two pinned layers are opposite direction and fixed. In this paper, TPL (pinned 1) is parallel to the free layer when the state is assigned to 1 and BPL (pinned 2) is parallel to the free layer when the state is assigned to 0. The proposed structure of Penta MTJ [13]needs less current for writing as compared to the conventional MTJ. It requires only current for converting antiparallel to parallel state for one stack, the other stack is automatically comes into antiparallel state. Moreover, the effect of process variation of one stack is nullified by another stack and in case of Penta MTJ[13] contrary to two different MTJs, whose the process Variations degrade the performance[14]. Actually, there is no experimental data is available for the double barrier and hence, we have assumed that single barrier model is also valid for a double barrier for TMR ratio.

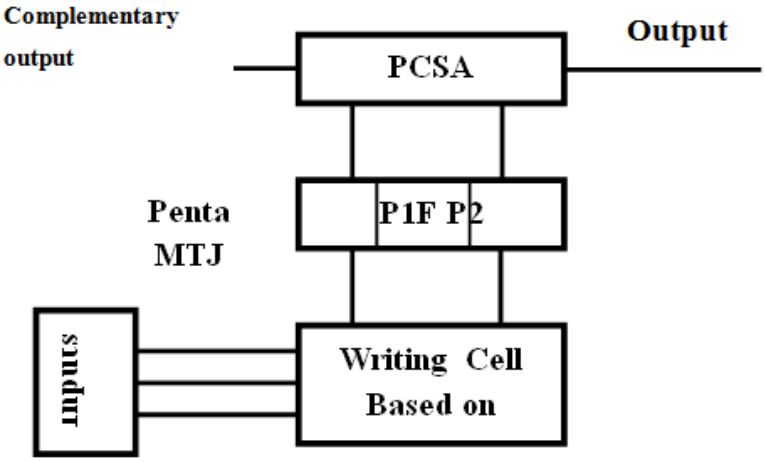

Fig 6.Block diagram of logic gates using Penta MTJ.

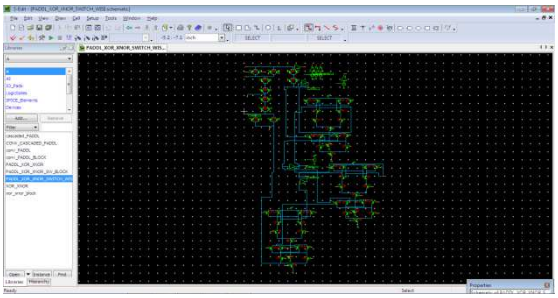

Fig7.circuit for switching diagram using penta MTJ

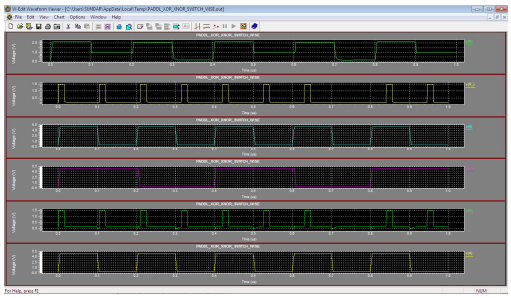

Fig 8.simulation results for switching diagram using penta MTJ

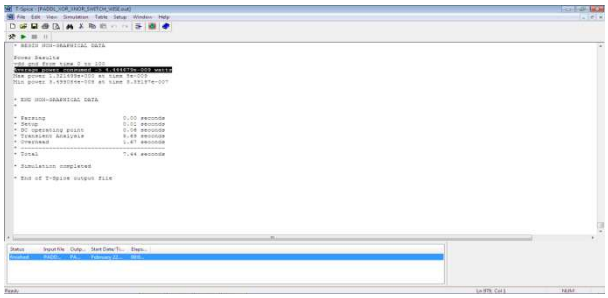

Fig 9.power consumption of switching diagram using penta MTJ

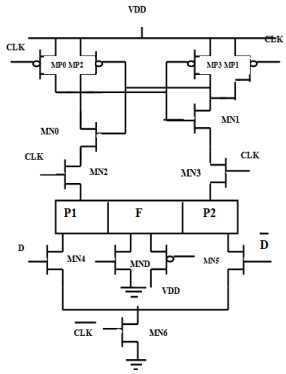

Fig 10. Writing, state detection, and amplification using PCSA of Penta MTJ cell

5 LOGICS IN MEMORY

In penta MTJ has three major important parts such as 1) PCSA (precharge sensing amplifier),2) penta MTJ logic and 3) penta MTJ writing cell. PCSA has two different phases such as precharge phase and evolution phase. The low read disturbance and dynamic sensing capability of an penta MTJ can reduces the delay. During precharging, CLK is low which disconnects the upper half from the lower half, i.e., precharging of PCSA at the time of writing leads to less delay as well as improved design. The PentaMTJs writing operation is done only one direction (from antiparallel to parallel state). Hence, the PCSA is discharging in only happens through the Penta MTJ and not through the writing transistors.

6 LOGIC GATES USING PENTA MTJ

The combinational and sequential circuits are building by logic gates. It is act as basic building blocks of Penta MTJ. The basic structure of Penta MTJ based logic gate is divided into three parts, as shown in fig.3(a) and described in section II.Fig.3(b) shows the based logic gates of penta MTJ.The different logic gates are required different writing circuitry but its sensing portion is remains identical.Hence,the information is saved in the pinned layer using series or parallel combinational of the transistor as the logic. The storing logic information of penta MTJ is designed such as for storing1,all logic combinations with high output are combined and the net expression is evaluated using K -map and for storing 0, the complement of the expression is evaluated. Fig. 6 shows the simulation results of logic gates. The A and B are the two inputs and its output 0 means discharging of PCSA where as 1 means no discharching of PCSA for the normal output. The evaluation phase begins after precharging the outputs of the PCSA to VDD using the clock CLK.

7 RESULT AND DISCUSSION

Using penta MTJ, the self-referencing property of the Penta MTJ is useful in decreasing the area overhead because of its differential nature. The switching current density in PMA is directly proportional to the magnetization, anisotropy field, and the thickness of the free layer. The thermal stability factor of MTJ/Penta MTJ governs the data retention capability of the digital logic. As compared with CMOS logic, the proposed magnetic logic gates consume more power and delay in writing but this logic gate consumes little static power which is a major power contributor along with the interconnect power at the Nanoscale.

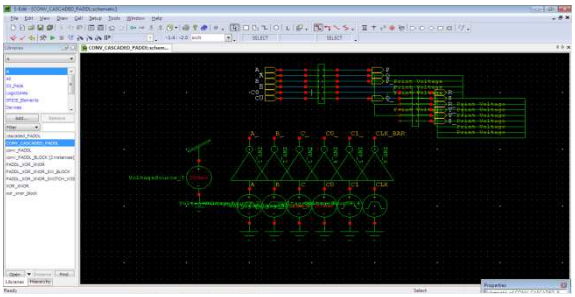

Fig 11. Circuit diagram for cascaded PADDL using conventional CMOS

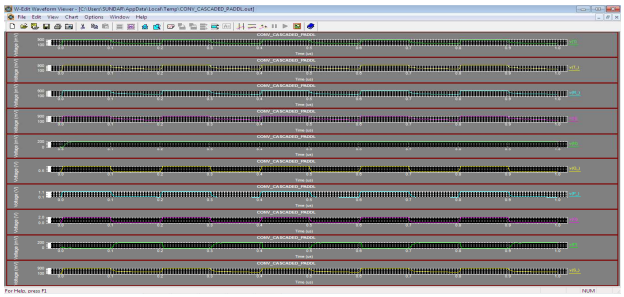

Fig 12.simulation results for cascaded PADDL using conventional CMOS

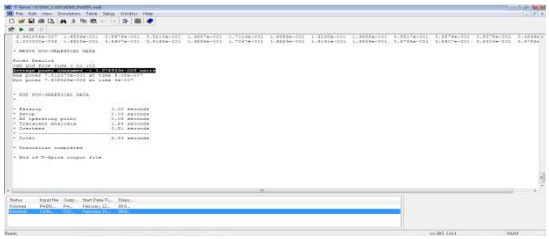

Fig 13.power consumption of conventional cascaded PADDL

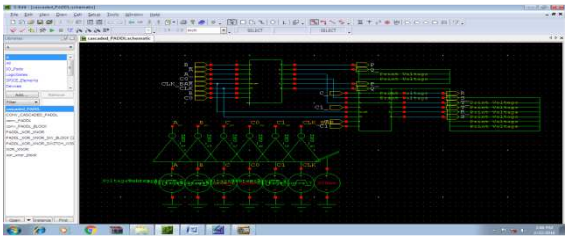

Fig.14 Circuit diagram for cascaded PADDL using penta MTJ

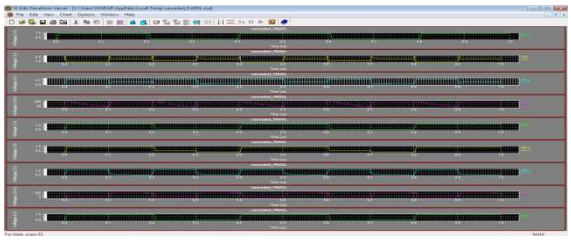

Fig.15 simulation results for cascaded PADDL using penta MTJ

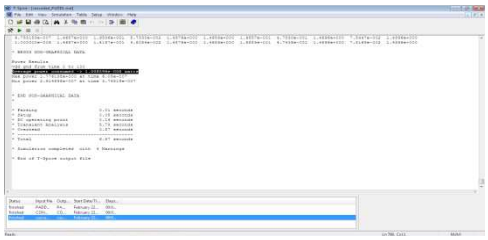

Fig.16 power consumption for cascaded PADDL using penta MTJ

CONCLUSION

In PADDL memory cell is constructed using conventional xor/xnor CMOS logic for reducing power consumption and delay but it is not achieved by using conventional xor/xnor CMOS logic. So that we are preferring penta MTJ –based CMOS logic for reducing power consumption and delay. In PADDL memory cell has almost all gate operations in it, so that we are using this memory cell in penta MTJ for easy cascading, self synchronization, less voltage headroom and better performance. The attractive features of MTJ/Penta MTJ-based CMOS logic are low static power, short interconnect delay and effective power gating because of non-volatility. Penta MTJ-based logic decreases the area overhead by removing the intermediate circuitry needed for conversion of voltage to current or current to voltage. Moreover, no initial condition is required for performing the logic operation and self referencing property removes the extra MTJs used for referencing. Penta MTJ also provides guaranteed disturbance free reading and increased tolerance to process variations due to its differential nature.

REFERENCES

[1] Dinesh Kumar T.R et al.2016, Design Of Adiabatic Dynamic Differential Logic For DPA-Resistant Secure Integrated Circuits Using Penta Mtj. Int J Recent Sci Res. 7(2), pp. 9075-9079.

[2] S.Tehraniet al., “Recent developments in magnetic tunnel junction MRAM,” IEEE Trans. Magn., vol. 36, no. 5, pp. 2752–2757, Sep. 2000.

[3] G. A. Prinz, “Magnetoelectronics,” Science, vol. 282, pp. 1660–1663, Nov. 1998.

[4] ERD. (2011). International Roadmap for Semiconductor (ITRS).
[Online] Available: http://www.itrs.net/Links/2011ITRS/Home2011.htm

[5] S. Parkin, X. Jiang, C. Kaiser, A. Panchula, K. Roche, and M. Samant, “Magnetically engineered spintronic sensors and memory,” Proc. IEEE, vol. 91, no. 5, pp. 661–680, May 2003.

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

[7] C. Chappert, A. Fert, and F. N. Van Dau, “The emergence of spin electronics in data storage,” Nature Mater., vol. 6, no. 11, pp. 813–823, Nov. 2007.

[8] S. D. Pable and M. Hasan, “Interconnect design for subthreshold circuits,” IEEE Trans. Nanotechnol., vol. 11, no. 3, pp. 633–639, May 2012. [8] H.-P. Trinh, W. Zhao, J.-O. Klein, Y. Zhang, D. Ravelsona, and

[9] Chappert, “Magnetic adder based on racetrack memory,” IEEE Trans.Circuits Syst. I, Reg. Papers, vol. 60, no. 6, pp. 1469–1477, Jun. 2013.

[10] J. S. Friedman, N. Rangaraju, Y. I. Ismail, and B. W. Wessels, “A spin-diode logic family,” IEEE Trans. Nanotechnol., vol. 11, no. 5, pp. 1026–1032, Sep. 2012.

[11] P. Horowitz and W. Hill, The Art of Electronics. Cambridge, U.K.: Cambridge Univ. Press, 1989.

[12] S. Huda and A. Sheikholeslami, “A novel STT-MRAM cell with disturbance-free read operation,” IEEE Trans. Circuits Syst. I, Reg.Papers, vol. 60, no. 6, pp. 1534–1547, Jun. 2013.

[13] W. Xu, T. Zhang, and Y. Chen, “Design of spin-torque transfer mag-netoresistive RAM and CAM/TCAM with high sensing and search speed,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 18, no. 1, pp. 66–74, Jan. 2010.

[14] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, “The EM side—Channel(s),” in Cryptographic Hardware and EmbeddedSystems. London, U.K.: Springer-Verlag, 2003, pp. 29–45.

[15] P. C. Kocher, “Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems,” in Advances in Cryptology. London, U.K.: Springer-Verlag, Aug. 1996, pp. 104–113.

[16] C. Clavier, J.-S. Coron, and N. Dabbous, “Differential power analysis in the presence of hardware countermeasures,” in Cryptographic Hardwareand Embedded Systems. London, U.K.: Springer-Verlag, Aug. 2000,pp. 252–263.

[17] P. Kocher, “Differential power analysis,” Advances in Cryptology (Lecture Notes in Computer Science), vol 1666. Berlin, Germany:Springer-Verlag, 1999, pp. 388–397.

[18] PTM 22 nm HSPICE Model. [Online] Available: http://ptm.asu.edu/modelcard/HP/22nm_HP.pm, accessed Jul. 15, 2013.

[19] L. N. Ramakrishnan, M. Chakkaravarthy, A. S. Manchanda,M.Borowczak, and R. Vemuri, “SDMLp: On the use of complementary pass transistor logic for design of DPA resistant circuits,” in Proc.IEEE Int. Symp. Hardw.-Oriented Security Trust (HOST), Jun. 2012,pp. 31–36

[20] K. Tiri and I. Verbauwhede, “A logic level design methodology for a secure DPA-resistant ASIC or FPGA implementation,” in Proc. DATE, 2004, pp. 246–251.

[21] V. Sundaresan, S. Rammohan, and R. Vemuri, “Power invariant secure-IC design methodology using reduced complementary dynamic and differential logic,” in Proc. IFIP Int. Conf. Very Large ScaleIntegr. (VLSI-SoC), Oct. 2007, pp. 1–6.