International Journal Of

Recent Scientific Research

ISSN: 0976-3031

Volume: 7(2) February -2016

DESIGN OF ADIABATIC DYNAMIC DIFFERENTIAL LOGIC FOR DPA-RESISTANT SECURE INTEGRATED CIRCUITS USING PENTA MTJ

Dinesh Kumar T.R., Priya M., Priyanka V., Ruby T and Anto Bennet M

THE OFFICIAL PUBLICATION OF
INTERNATIONAL JOURNAL OF RECENT SCIENTIFIC RESEARCH (IJRSR)
http://www.recentscientific.com/ recentscientific@gmail.com

Available Online at http://www.recentscientific.com

ISSN: 0976-3031

International Journal of Recent Scientific Research
Vol. 7, Issue, 2, pp. 9075-9079, February, 2016

International Journal of Recent Scientific Research

RESEARCH ARTICLE

DESIGN OF ADIABATIC DYNAMIC DIFFERENTIAL LOGIC FOR DPA-RESISTANT SECURE INTEGRATED CIRCUITS USING PENTA MTJ

Dinesh Kumar T.R., Priya M., Priyanka V., Ruby T and Anto Bennet M

Department of Electronics and Communication Engineering, Veltech, Chennai-600062

ARTICLE INFO

Article History:

Received 15th September, 2015
Received in revised form 21st November, 2015
Accepted 06th January, 2016
Published online 28th February, 2016

Keywords:

high-performance adiabatic dynamics differential logics (PADDL), Differential power Analysis (DPA) Attack, Penta MTJ, Magnetic tunnel junction, Magneto resistance.

ABSTRACT

In this paper 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). This methodology suitable for integration in a common automated standard cell ASIC or FPGA design flow. For stronger mitigation of DPA attacks, we proposed this design and analysis using high-performance adiabatic dynamic differential logic (PADDL) for mitigating DPA attacks for applications in secure integrated circuit (IC) design. A Penta MTJ-based gate that provides simple cascading, self-referencing, less voltage headroom downside in pre charge sense electronic equipment and low space. These types of gate will be implemented in (PADDL).For different logic gates and different writing circuitry is required but the sensing portion is remains identical. Therefore, the information is stored in the pinned layers using series or parallel combinations of transistors as per the logic storing in PentaMTJ. The logic gate is validated by simulation at the 22nm technology node using a tanner tool.

INTRODUCTION

SMART cards are any pocket-sized card that has embedded circuits. Smart cards are made of plastic or tokens. it may provide 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 use a tamper resistant securefile 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[2].

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[1] the amount of time required to perform private-key operations [3] and analysis of noisy power consumption [4]. In this the most effective attack is Differential Power Analysis attack (DPA) [5], 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

Corresponding author:* **Dinesh Kumar T.R
Department of Electronics and Communication Engineering, Veltech, Chennai-600062

absence of electric charge in terms of voltage VDD or GND. But in Spintronics up and down spin of electrons. In recent, researchers have developed a spintronic devices, such as magnetic tunnel junctions (MTJs), which is operates in the principle of tunnel magneto resistance (TMR)[6]. An MTJ is made of two ferromagnetic layers separated by an oxide layer. To improve the performance of CMOS logic circuit in terms of power dissipation, area required, and interconnection delay. It also can be easily fabricated using 3-D backend integration process, which is compatible with CMOS process, without any area overhead.

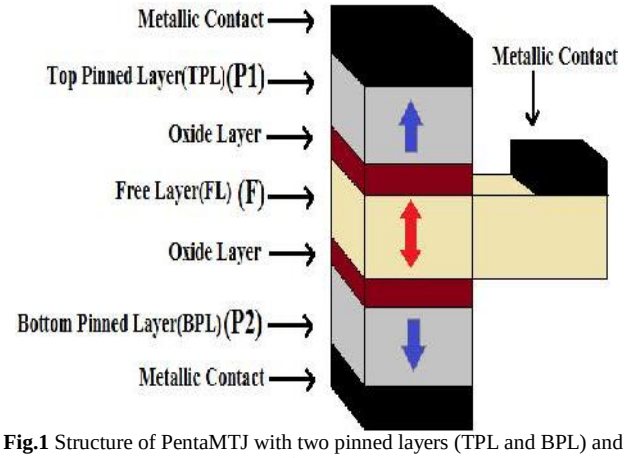

Fig.1 Structure of PentaMTJ with two pinned layers (TPL and BPL) and one free layer.

MTJ has dual properties such as processing and storage. It is help to reduce the memory and interconnect delay/power [14] are needed to store the processed data back into memory. In [7]a magnetic XOR gate is comprising of six MTJs and the transistors is presented. The area requirement is less but the number of MTJ increases and the writing energy also increases, which is a serious limitation of the hybrid circuit consisting of MTJ and CMOS. Friedman *et al*.[8] and Horowitz and Hill[9] 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 Nanoscale, respectively.

MOTIVATION AND BACKGROUND

A. Secure Integrated Chip Design

Secure integrated chip used in a smart cards, which contains the arithmetic logic unit, mainprocessor, processingregisters, read-only memory(ROM) for storing the operating system, random access memory(RAM) for arithmetic processing and electrically erasable programmable ROM for data memory. The operating system controls the data access and to implement the cryptographic security algorithms. The international standard for contact smart card is ISO/IEC 7816 [2]and the contactless smart card is ISO/IEC 14443[11].In this standard, triple data encryption standard (DES) used in the smart cards and the operating frequency is 13.56 MHZ.

B. DPA Attacks

In software systems security and hardware oriented security requires a two prong approach to smart card security. Smartcard 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, radiofrequencies, 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.

C. 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.

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[13].

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.

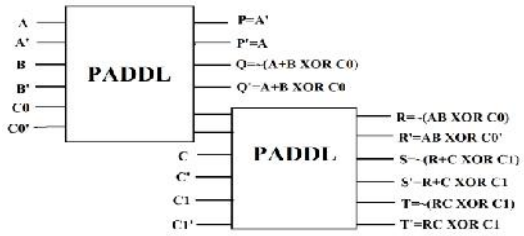

Fig.2 Cascaded PADDL cells with logic outputs shown

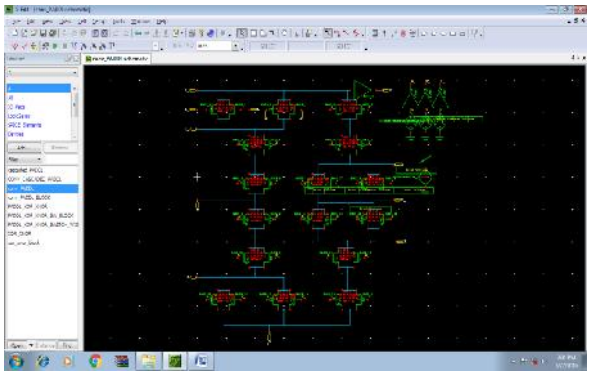

Fig 3 Conventional PADDL schematic diagram

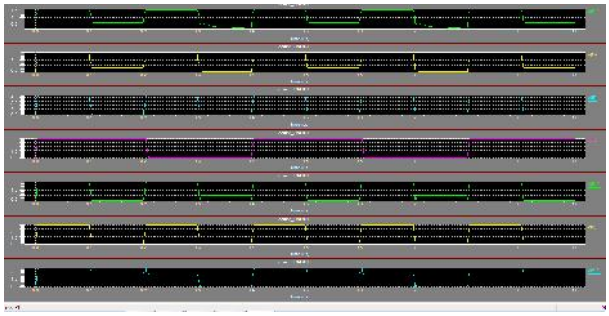

Fig 4 Simulation result for convential PADDL

The first design is a PADDL, which is optimized for very high operating frequencies. This design improves upon previously presented benchmarks [15] by 76.41% for average power due to a reduced reliance of evaluation discharge network.

The PADDL cell also improved upon the differential power of a conventional NAND gate by a factor of 112.The attractive features of MTJ/pentaMTJ based CMOS logic are low static power, short inter connect delay, and effective power gating because of nonvolatility. PentaMTJ also provides guaranteed disturbance free reading and increase tolerance to process variations due to its differential nature.

Table 1 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

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 PentaMTJ [11]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 PentaMTJ[11] contrary to two different MTJs, whose the process Variations degrade the performance[12]. 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.

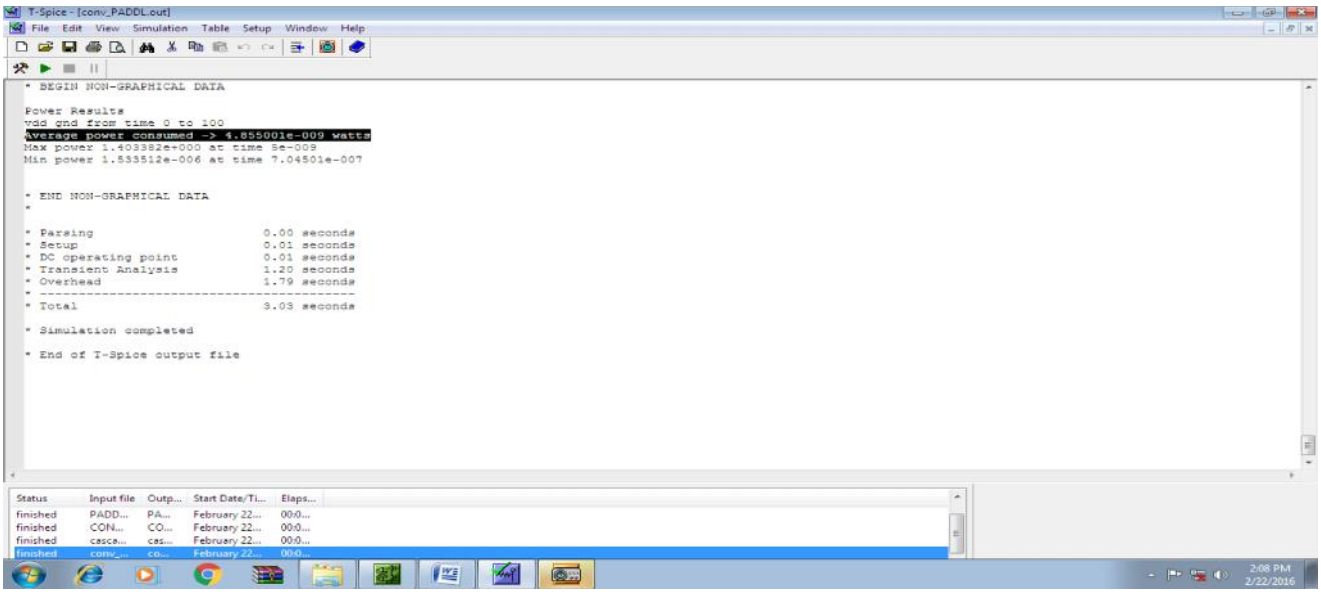

Fig 5 Estimation of power for conventional PADDL

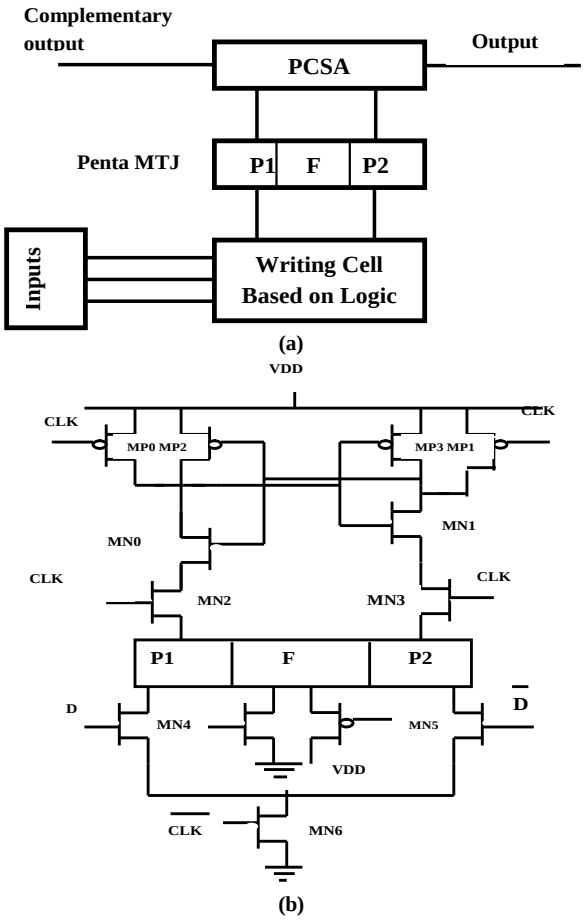

Fig.3 (a) Block diagram of logic gates using PentaMTJ. (b) Writing, state detection, and amplification using PCSA of PentaMTJ cell.

The pentaMTJ has lower resistance than the conventional MTJ because it works well for small value of oxide thickness [11].

Logics In Memory

In pentaMTJ has three major important parts such as 1) PCSA (precharge sensing amplifier), 2) pentaMTJ logic and3) pentaMTJ writing cell. PCSA has two different phases such as precharge phase and evolution phase. The low read disturbance and dynamic sensing capability of an pentaMTJ 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 PentaMTJ and not through the writing transistors.

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 PentaMTJ 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 pentaMTJ. 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 pentaMTJ 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. 4 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.

RESULT AND DISCUSSION

Using pentaMTJ, the self-referencing property of the PentaMTJ 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/PentaMTJ 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

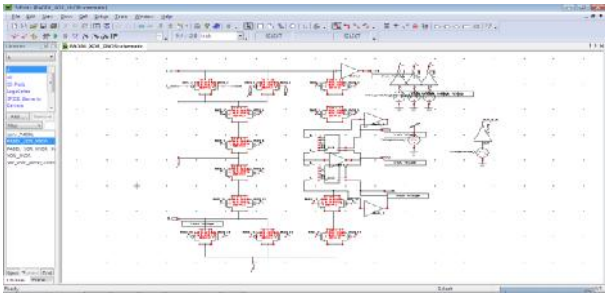

Fig5 PADDL XOR/XNOR schematic Diagram

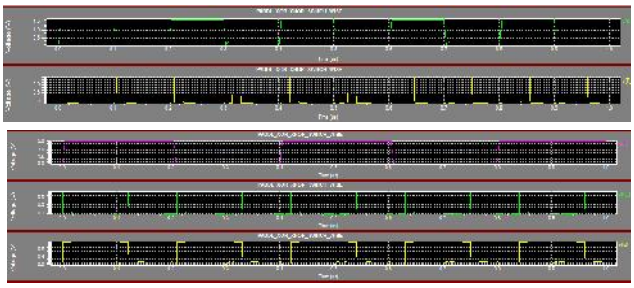

Fig 6 simulation result for PADDL XOR/XNOR schematic

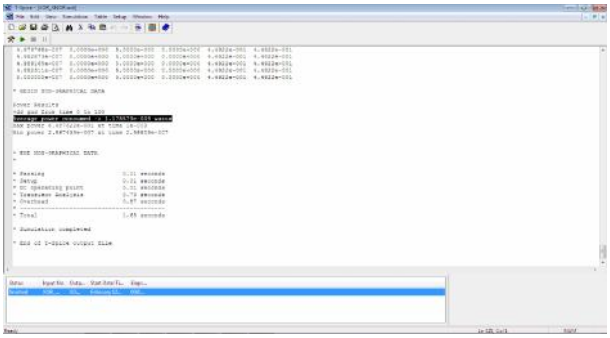

Fig 7 Estimatiion of power for PADDL XOR/XNOR Schematic

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 pentaMTJ –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 pentaMTJ for easy cascading, self synchronization, less voltage headroom and better performance.

The attractive features of MTJ/PentaMTJ-based CMOS logic are low static power, short interconnect delay and effective power gating because of non-volatility. PentaMTJ-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. PentaMTJ also provides guaranteed disturbance free reading and increased tolerance to process variations due to its differential nature.

References

1. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM side—Channel(s)," in Cryptographic Hardware and Embedded Systems. London, U.K.: Springer-Verlag, 2003, pp. 29–45.
2. 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.
3. 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.
4. P. Kocher, "Differential power analysis," Advances in Cryptology (Lecture Notes in Computer Science), vol 1666. Berlin, Germany: Springer-Verlag, 1999, pp. 388–397.
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. H.-P. Trinh, W. Zhao, J.-O. Klein, Y. Zhang, D. Ravelsona, and C.Chappert, "Magnetic adder based on racetrack memory," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 60, no. 6, pp. 1469–1477, Jun. 2013
7. 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.
8. 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.
9. 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.
10. S. D. Pable and M. Hasan, "Interconnect design for subthreshold circuits," IEEE Trans. Nanotechnol., vol. 11, no. 3, pp. 633–639, May 2012
11. 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.
12. 8.Dr. AntoBennet, M, Sankar Babu G, Suresh R, Mohammed Sulaiman S, Sheriff M, Janakiraman G, Natarajan S, "Design & Testing of Tcam Faults Using T_H Algorithm", *Middle-East Journal of Scientific Research* 23(08): 1921-1929, August 2015 .
13. 9.Dr. AntoBennet, M "Power Optimization Techniques for sequential elements using pulse triggered flipflops", *International Journal of Computer & Modern Technology* , Issue 01 ,Volume01 ,pp 29-40, June 2015.
14. 10.Dr. AntoBennet, M, Manimaraboopathy M,P. Maragathavalli P, Dinesh Kumar T R, "Low Complexity Multiplier For Gf(2m) Based All One Polynomial", *Middle-East Journal of Scientific Research* 21 (11): 2064-2071, October 2014.
15. Dr. AntoBennet, M , Resmi R. Nair, Mahalakshmi V, Janakiraman G "Performance and Analysis of Ground-Glass Pattern Detection in Lung Disease based on High-Resolution Computed Tomography", *Indian Journal of Science and Technology*, Volume09 (Issue02):01-07, January 2016

****

How to cite this article:

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.

TSSN 0976-3031