International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

A Novel Architecture for Low Power Adiabatic Cipher

Samik Samanta, Rajat Mahapatra, Ashis Kumar Mal

Abstract: ***AES stands for Advanced Encryption Standard. It is widely used in today's various security applications. S-box method is the most common and important in today's data security and embedded applications.. This S-box consumes a considerable percentage of power of the whole system. S-box is very prone to differential power attacks(DPA). DPA is the most threatening types of attacks in cryptographic systems. In this paper, we have implemented one positive polarity Reed Muller type S-box is implemented using adiabatic logic. Efficient charge recovery logic(ECRL)is used here. FinFET based ECRL is used to implement the S-box has been observed and calculated .The performance of ECRL based S-box is compared with conventional CMOS based S-box. The statistical parameters for DPA cipher design are also analyzed.***

Index Terms: Adiabatic, FinFET, CCS, SCRL, power clock.

I. INTRODUCTION

Minimizing the power consumption of systems and processes is one of the primary concern in today's circuit design .Modern age is the age of security and wearable embedded computing. Data security in cyber networks and systems is a modern issue of research. This is a mixture of various techniques and computing methods. that protects the networks or networked systems from various hazards and damages. All these damages and hazards are initiated by cyber hackers. To avoid these damages, there are various standard encryption techniques which are available and used in cyber security industries. Advanced Encryption Standard (AES) is a widely used among them. This is a symmetric encryption technique. The main element of AES hardware is S-box. Differential power analysis (DPA) generally makes severe attacks on S-boxes [2]. During the process execution, the power consumption of cryptographic systems is not constant. Generally, statistical correlation method is used in DPA to recover the information from the noised portion. DPA systems have high power consumptions. Various measures are discussed in literature and already available in literature to overcome high power consumption in DPA. Among them, the most secure, reliable and effective design technique is to use adiabatic logic or energy recovery logic based S-box architectures. Various devices also available for S-box hardware. Among various devices available Fin field effect transistor (FinFET) is the most effective device for implementation of S-box. Another advantage is that, this can also minimize the leakage current of the system. The modern age is the age of system on chip (SoC), Internet of Things (IoT) and wearable computing. So there is an increasing demand for low power high security computing devices. For Internet of Things devices or applications or wearable devices to perform smoothly, it requires a battery as main power source [3]. So battery life is primary design concern of battery operated computing devices and systems. These computing devices operate at low frequencies. In low frequencies adiabatic logic can perform well with low power dissipation. They are taken as key devices or heart for main system in low power computing and security systems and devices (ciphers).

II. ADIABATIC LOGIC

The term adiabatic comes from a Greek word 'adiabatos'. It means a reversible thermodynamic process. This process occurs without gain or loss of energy or power. The traditional power source that is generally used by conventional CMOS logic circuits is not taken into account by adiabatic systems. They are also called energy recovery systems. These energy recovery circuits use power supply and clock using same bus that is called power clocks [5]. The use of power clock enables efficient recycling of the charge stored in load capacitor. The technique of power or energy recycling has a limitation. The process limits the dynamic switching based energy loss. This dynamic loss contributes 85-90% of total power consumption Energy recovery circuits utilize a constant current source (CCS). But a constant voltage source (CVS) is used by the conventional circuits. The basic charging and discharging cycles of adiabatic logic are shown in Fig. 1

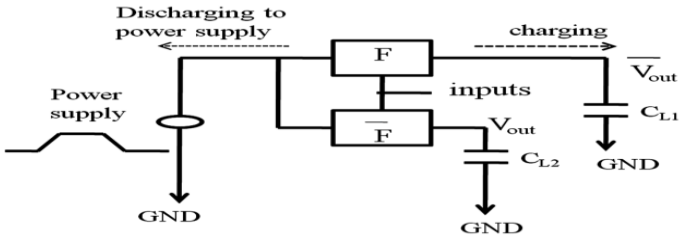

Fig. 1. Basic adiabatic charging and discharging cycle

Manuscript published on November 30, 2019.
* Correspondence Author
Samik Samanta*, ECE Department, Neotia Institute of Technology, Management &Science, India
Rajat Mahapatra, ECE Department, National Institute of Technology, Durgapur, India
Ashis Kumar Mal, ECE Department, National Institute of Technology, Durgapur, India

The energy dissipated in an adiabatic circuit driven by a constant current source is given in Eq. 1.

$$E_d=RC/T \times CV_{dd}^2 \quad (1)$$

The adiabatic losses also show the relationship with RC time constant. That is shown in Eq. 2.

$$E_d= R_{on}C/T \times CV_{dd}^2 \quad (2)$$

Where R_{on} is the on resistance of the device. Equation.3 shows the relationship of non adiabatic losses with voltage. The non adiabatic losses of a circuit are independent of operating frequency. The non adiabatic loss can be expressed as

$$E_{non\text{-}ad} = 1/2\ CV_{th}^2 \quad (3)$$

There is a leakage loss which contributes nearly 10% of total losses in adiabatic circuits. This is due to scaling or rapid minimization of transistors parameters. This can also be caused due to improper transistor sizing. The leakage loss can be expressed in equation 4.

$$E_{leakage} = V_{dd}.I_L/f \quad (4)$$

Where I_L is the leakage current and f is the power supply frequency.

Adiabatic switching utilizes charging and discharging of nodes in a very slow process. In this method the output capacitor is used to load and unload the power. This is achieved by the use of dynamic or switching power source. In semiconductor industry, various types of adiabatic circuits are available. These circuits are classified in basic two types. They are fully adiabatic or semi adiabatic logic. This is based on the nature of power dissipation of the logic. Some examples of quasi adiabatic type of logic may be given like positive feedback adiabatic logic (PFAL), efficient charge recovery logic (ECRL), clocked adiabatic logic (CAL) [5]. Some examples of fully adiabatic logic are pass transistor adiabatic logic (PAL), split rail charge recovery logic (SCRL). Adiabatic logic can be applied to security applications depending on some parameters like power dissipation and design complexity. The circuit complexity of adiabatic systems can be measured in terms of number of devices, structure of power supply that is power clocks, efficiency and system reliability. These are the limitations of the secure adiabatic logic families. The ECRL family matches all these parameters. Therefore, this is the best choice for data security applications based on adiabatic S-box structure. Generally, MOSFETs suffer from the short channel effects when the channel length is comparable to the depletion layer widths of the source and drain junctions. This short channel effects (SCEs) are reduced in Fin FET transistors.

Moreover, the FinFET transistors show very low leakage current and very high on-state current [11]. Due to high on state current, these devices provide very fast switching speed. In these devices the leakage current is also found to be very negligible. FinFET is a multi gate structure [7]. The multi-gate nature of FinFET allows it to be operated in multiple modes. Various modes are named as independent gate mode, shorted gate mode and low-power mode. The basic structure of FinFET is presented in fig2.

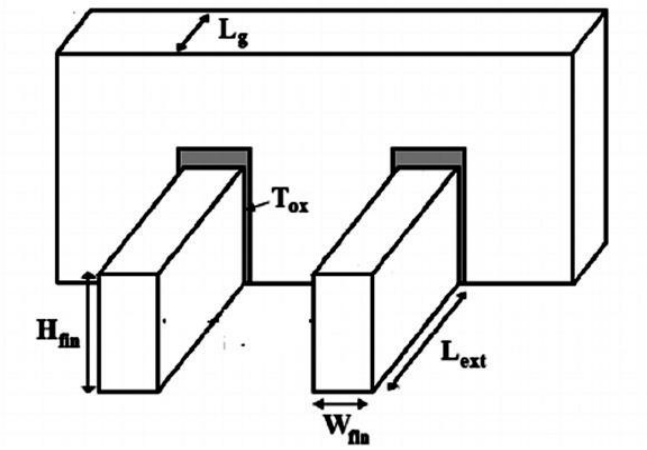

Fig. 2. Basic FinFET structure with length, height and thickness

III. AES AND S-BOX

AES stands for "Advanced encryption standard". This structure is designed based on Rijndael algorithm .This is nothing but one type of data encryption standard. The basic criteria of a security based algorithm are that the algorithm should have highest security, better performance, and higher efficiency and good redundancy. AES is one of the widely used algorithms in various modern low power applications. The applications are not limited to wearable devices, date protection, switching in networks, wireless sensor networks and internet of things. The efficiency of AES hardware depends on its basic architecture. The AES implementation is clearly identified in Fig. 3.

There are two basic methods for S-box circuit implementation. These two methods are used and implemented widely. The first method is the construction of multiplicative inverse and affine transform in an independent manner. and after that connecting them serially. The advantage of this process is that it reduces area. This is achieved by composite field arithmetic. The second method is the construction of a single circuit unit. In this technique, S-box is implemented from truth table. The table is called look up table of LUT [9]. The table has some terms of digits exactly same like Boolean model of digital circuits. It is expressed as the sum of products, product of sums (PoS), and positive polarity Reed Muller block. The efficiency of these two methods can be compared. From comparison, it can be found that the PPRM S-box consumes very high power compared to composite field S-box [9]. The cause is that, there is large number of signal transition probabilities that occur in this method. This increases number of switching activities per node. This adds to total power consumption. This power consumption problem can be overcome and minimized. This is achieved by considering three sub-components of composite field S-box. After that the designer has to convert them to PPRM form. The stages can be termed as, the pre-inversion, inversion and post-inversion sections. Each of them is implemented with two-level AND and XOR arrays and reduces the signal transition probability.

This design architecture thus achieves a good and efficient utilization of power sources. There is no extra wastage of power of the system in this method. This PPRM has another name. It is called zero polarity form (ZPF). This is a XOR sum of products. In this method each variable is in un-complemented form.

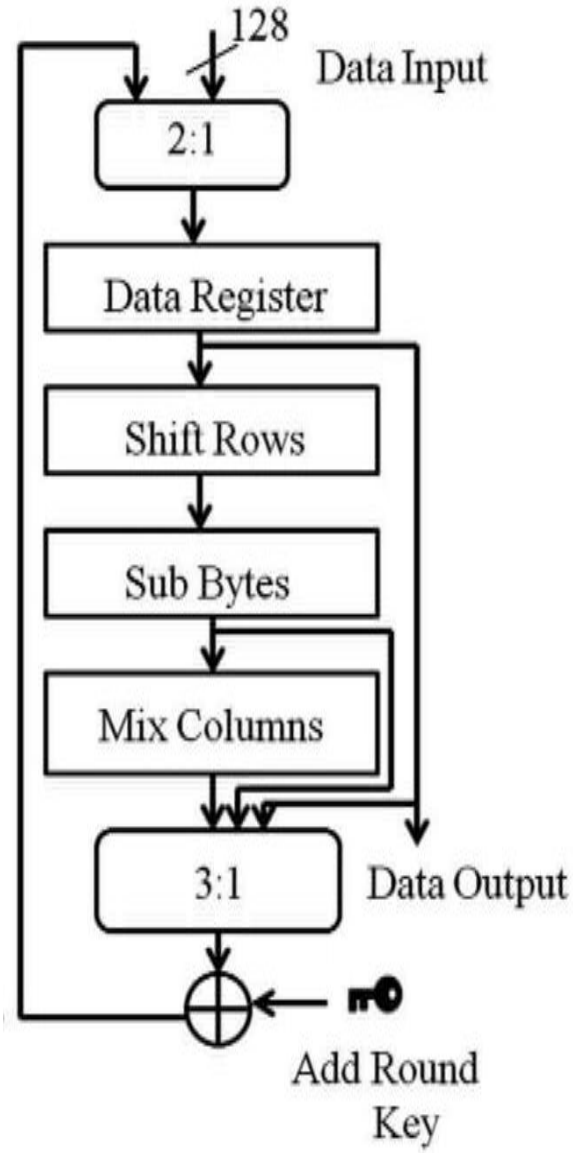

Fig.3. Block diagram of AES method

IV. FINFET IMPLEMENTATION

We have implemented the two-input ECRL AND/NAND, XOR/XNOR gates using FinFET. These are shown in Fig. 4. The front gate of the FinFET is used as input. The back gate of P FinFET is connected to power supply or in adiabatic circuits, this is termed as power clock denoted by Vpc and N FinFET to ground. This is generally for low power consumption. The transition probability of the output depends largely upon the input in conventional gates. A control signal 'S' is used to remove the data dependency. Here X and Y are dual inputs. OUT and OUTb are the outputs. These are with Vpc as four-phase power clock supply. The four phases are charging, evaluation, hold and recover. This provides power supply signals and clock signals.

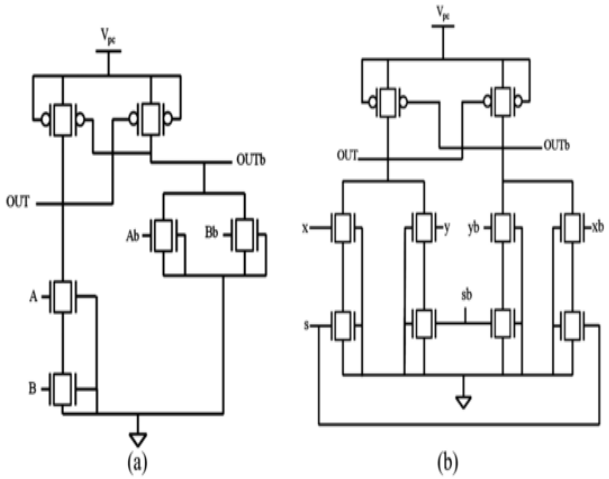

Fig. 4.(a) ECRL based AND/NAND .(b) XOR/XNOR gates

The simulation results are shown for ECRL AND/NAND gate is shown in Fig. 5. The circuit has dual inputs A, B and outputs OUT and OUTb. For ECRL XOR/XNOR gates simulation is shown in fig 6.The current trace plot of the circuit shows same peak value of current and also exhibits uniform low-power dissipation for different input transitions.

V. SIMULATION RESULTS

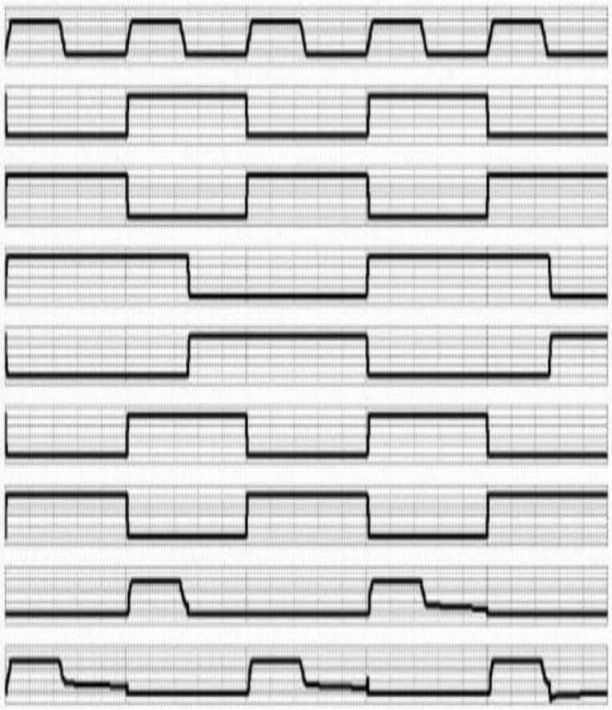

Fig. 5. ECRL based AND/NAND simulation results

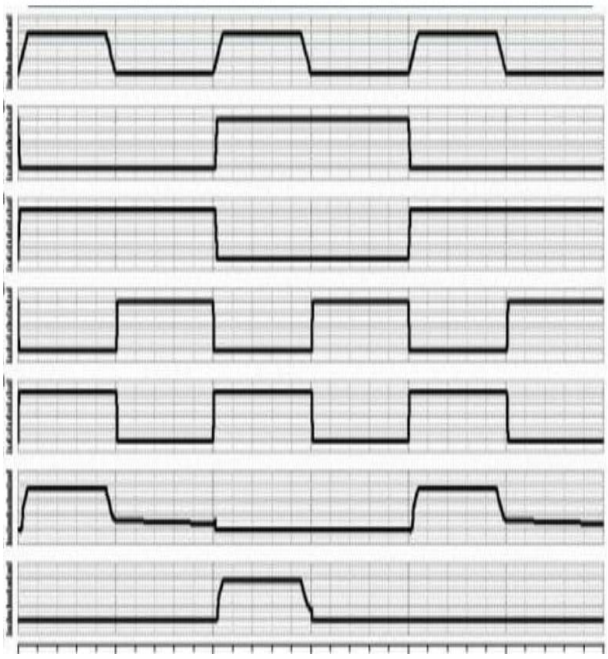

Fig. 6. ECRL based XOR/XNOR simulation results

The structure given will ensure a uniform peak current for the input transitions. Thus there is very less probability for the hacker to predict the input data.

Table 1. Comparison of no. of components and area.

Transistor/Area	CMOS	FinFET
No. of PMOS	1878	798
No. of NMOS	1878	2010
Area	0.0167	0.0029

Table 1. shows the no. of transistors in CMOS and FinFET implementation. It is clearly found that FinFET structure has less number of components that CMOS implementation. The area for CMOS and FinFET have also been calculated. This is also easily noticed that FinFET has minimum area than equivalent CMOS structures.

Table 2. Comparison of S-box performance

Parameter	CMOS	FinFET
Power	11.28µW	5.61 µW
Delay	1.19ns	1.21ns

Table 2 shows the power dissipation and delay of CMOS and FinFET structure. It can be easily found that CMOS has high power that FinFET structure. The delays of both the circuits are nearly same

Table 3. Comparison of parameters using various microelectronic technologies at 1MHz.

Technology	MOSFET	FinFET
250nm	80.11 µW	16.31ns
180nm	41.01 µW	5.81ns
90nm	11.18 µW	3.47ns
45nm	7.61 µW	1.17ns

In Table 3. We have estimated the power dissipation of MOSFET and FinFET in various technologies. It can be easily found that in all the technologies, FinFET structure has minimum power dissipation.

There is a statistical analysis of normalized energy to find out the robustness against DPA attacks. The parameters for DPA analysis are normalized energy deviation (NED) and normalized standard deviation (NSD). These two parameters determine the ability of the design structure against power analysis attacks which depends on input transitions.

$$NED = E_{max}-E_{min}/E_{max} \quad (5)$$

$$NSD = €/E_1 \quad (6)$$

E_{max} and E_{min} are the maximum energy, minimum energy. The parameter NED shows the difference in maximum and minimum energy levels irrespective of input transitions. Similarly, NSD determines the similarity of various energy level transitions concerning mean energy level. Lowest values of NSD and NED indicate the ability of the logic against DPA attacks.

Table 3. Calculation of statistical parameters

Frequency	NED	NSD
10MHz	8.28µW	10
20MHz	11.19 µW	15
40MHz	22.78 µW	18

Table 3 shows the values of statistical parameters NED and NSD.

Table 4. Comparison of power dissipation with voltage in 1MHz

Voltage	CMOS	FinFET
1V	25.1µW	15.9 µW
0.7V	13.1 µW	8.2 µW
0.2V	1.5 µW	0.02 µW

Table4. shows the power dissipation of CMOS and FinFET based S-boxes. This is very clear that FinFET box S-box has very minimum power dissipation over CMOS S-box.

VI. SIMULATION RESULTS

From all the simulation results and parameter calculated values, it is found that FinFET –ECRL based S-box in very robust against the DPA attacks. This circuit has very large values of NED and NSD. These two are the main statistical parameters for analyzing DPA attacks. These high values of NES and NSD parameters indicate that the FinFET-ECRL based S-box is very efficient. Moreover, this implemented S-box has minimum area and good area efficiency. This type of adiabatic FinFET structures is very useful cyber security systems and wearable embedded applications.

VII. CONCLUSION

From all the simulation results and estimated values, it is clear that FinFET –ECRL based substitution box or S-box in very robust against the cyber or DPA attacks. This circuit has very large values of statistical parameters responsible for cyber attacks. The parameters known as NED and NSD has very high values. The high values of these parameters indicate that the FinFET-ECRL based S-box has very efficient security features in IOT and embedded applications. Moreover, this implemented S-box has other advantages also. It has minimum area overhead and good area efficiency. This type of adiabatic FinFET structures is very useful in ultra low power cyber security systems weable applications and IOT based gadgets.

REFERENCES

1. K.Lundager, B. Zeinali ,M. Tohidi, K. Madsen, and. ,F. Moradi "Low Power Design for Future Wearable and Implantable Devices", J. Low Power Electronics and Applications, Vol. 2, No. 26, pp. 1-26.
2. S.Sharma, "Performance analysis of inverter gate using FinFET and Planar bulk MOSFET technologies", International Journal of Electrical and Electronics Engineers, vol. 07, no. 01, Jan-June 2015, ISBN 2321–2055
3. Y.Moon, D.K.Jeong, "An efficient charge recovery logic circuit", IEEE J Solid-State Circuits, vol. 31, pp. 514-522, 1996.
4. 4.S.Samanta, R.Mahapatra, A.K.Mal " Analysis of adiabatic flip-flops for ulta low power applications" 3rd International Conference on devices for integrated circuits 2019" organized by KGEC, India
5. P.Kocher, J.Jaffe, and B.Jun, "Differential power analysis," in Advances in CryptologyCRYPTO99. Springer, 1999, pp. 388–397
6. C. Monteiro, T. Yasuhiro, and S. Toshikazu, "DPA resistance of charge sharing symmetric adiabatic logic.," in Proc. IEEE Int. Symp. Circuits Syst. (ISCAS), May 2013, pp. 2581–2584.
7. S.J.Park, D.Y.Jeon; Montès, L.Montes, Barraud, "Impact of channel width on back biasing effect in tri-gate MOSFET". Microelectronic. Eng. 2014, 114, 91–97.
8. P.Teichmann "Adiabatic Logic: Future Trend and System Level Perspective", Springer, Vol. 34, Edition 1, pp. 5-22. 2012
9. C.Monteiro Y.Takahashi, and T.Sekine " Low Power Secure AES S-box using Adiabatic Logic Circuit", Proc. of Faible Tension Faible Consummation (FTFC), pp. 1-4.
10. Paul Kocher, Joshua Jaffe, and Benjamin Jun (1999) Differential Power Analysis, Advances in Cryptology, LNCS, Vol. 1666, pp. 388–397.
11. Paul Kocher, Joshua Jaffe, Benjamin Jun, and Pankaj Rohatgi (2011) Introduction to Differential Power Analysis, The Journal of Cryptographic Engineering, Vol. 1, No. 1, pp. 5–27.
12. Hisamoto D., Wen-Chin Lee, J. Kedzierski, H. Takeuchi, K. Asano , C. Kuo, E. Anderson, Tsu-Jae King, J. Bokor, and Chenming Hu (2000) FinFET: A SelfAligned Double Gate MOSFET Scalable to 20nm, IEEE Trans. Electron Devices, Vol.47, No.12, pp. 2320–2325.
13. Sumio Morioka and Akashi Satoh (2002) Optimized S-box Architecture for Low Power AES Design, Proc. Int. Workshop on Cryptographic Hardware and Embedded Systems, 172-186
14. .J. Singh et al., "14 nm FinFET technology for analog and RF applications", Proc. IEEE Symp. VLSI Technol., pp. T140-T141, Jun. 2017.
15. C-H. Lin et al., "High Performance 14nm SOI FinFET CMOS Technology with 0.0174µm2 embedded DRAM and 15 Levels of Cu Metal", pp. 74-76, 2014.
16. K. Cheng et al., "Bottom oxidation through STI (BOTS)-A Novel Approach to Fabricate Dielectric Isolated FinFETs on Bulk Substrates", VLSI-Technology, 2014.

AUTHORS PROFILE

Samik Samanta, is associated with Neotia Institute of Technology, Management and Science, India. He has 16 years of teaching experience. His fields of interests are low power VLSI design, adiabatic logic and SoC design. He is also a research scholar of National Institute of Technology, Durgapur, India. He has already published many articles in many peer reviewed journals.

Rajat Mahapatra, is currently working as Professor in ECE department of National Institute of Technology, Durgapur. He has 16 years of teaching and research experience. His field of interests are VLSI device modelling, Low power VLSI design and resistive memory devices. He has worked as principal investigator in various funded projects. He has many publications in various peer reviewed journals.

Ashis Kumar Mal, is currently working as Professor and Head in ECE department of National Institute of Technology, Durgapur. He has more than 25 years of teaching and research experience. His field of interests are digitally assisted analog circuits, Analog and mixed signal VLSI and integer sequences. He has worked as principal investigator in various funded projects. He has many publications in various peer reviewed journals.