Journal of Science and Technology, Vol. 10 No. 3 (2018) p. 10-17

Ultralow-Power and Secure S-Box Circuit Using FinFET Based ECRL Adiabatic Logic

K. Srilakshmi[1*], A. V. N.Tilak[1] and K. Srinivasa Rao[2]

[1]Dept. of ECE, Gudlavalleru Engineering College, Gudlavalleru, Andhra Pradesh, India.
[2]TRR College of Engineering, Inole, Hyderabad, Telangana.

Received 14 April 2018; accepted 10 July 2018; available online 19 September 2018
DOI: https://10.30880/jst.2018.10.03.003

Abstract: Advanced Encryption Standard (AES) is the widely used technique in critical cyber security applications. In AES architecture S-box is the most important block. However, the power consumed by S-box is 75% of the total AES design. The S-box is also prone to Differential Power Analysis (DPA) attack which is one of the most threatening types of attacks in cryptographic systems. In this paper, a three-stage positive polarity Reed-Muller (PPRM) S-box is implemented with 45 nm FinFET using Efficient Charge Recovery Logic (ECRL) to reduce power consumption. The simulation results indicate up to 66% power savings for FinFET based S-box as compared to CMOS design. Further, the FinFET ECRL 8-bit S-box circuit is evaluated for transitional energy fluctuations and peak current traces to compare its resistance against side-channel attacks. The lower energy variations and uniform current trace exhibit the improved security performance of the circuit to withstand DPA and Differential Electromagnetic Radiation Attacks (DEMA).

Keyword: Cyber Security; Low-power; ECRL; FinFET; PPRM; S-box.

1. Introduction

Cybersecurity is a combination of various technologies and processes that protect the computing and networked systems from potential damage caused by hackers. One way to achieve security is by employing different encryption techniques. Advanced encryption standard (AES) [1] is one of the widely used symmetric encryption algorithms. The hardware of the AES is dominated by substitution box (S-box). The S-box is prone to differential power analysis (DPA) attack due to its large power consumption. The power consumption of cryptographic hardware is not constant during execution [2]. The simple power analysis recovers information directly by observation of the power consumption of a device [3], whereas the differential power analysis uses statistical correlations between the power consumption of the module and the input data [4] to recover the information.

Different countermeasures to DPA attacks are available in the literature [5], but they are not suitable to implement devices because power consumption is the major design constraint. Adiabatic logic is one of the low-power and secure design technique [6] due to its energy recovery principle.

The scaling of technology leads to threshold voltage reduction and consequent increase in leakage current. This will impact the energy recovery of the adiabatic logic circuits implemented using CMOS [7] and DPA attacks. Hence there is a need to investigate novel low-power and secure devices to be useful for these applications. Among different devices available, FinFET is the prominent device with reduced leakage current [8].

One of the significant challenges in today's electronic circuit design is lowering the power consumption of the computation. With the widespread use of internet of things (IoT), there is an increasing demand for low power and high-security devices. In General, the IoT devices are operated with a battery. So, battery life is the primary design consideration while designing battery operated systems. These devices are operated at low-frequency range, for example, the operating frequency of radio frequency ID (RFID) is 13.56 MHz [9]. Adiabatic logic circuits are proven to be effectively operated at these frequencies. Among different logic families, FinFET based ECRL adiabatic logic is chosen as it offers better energy savings [10]. The prime objective of this work is to design energy

*Corresponding author: slkaza06@gmail.com

e-ISSN: 2600-7924/penerbit.uthm.edu.my/ojs/index.php/jst

efficient three-stage Positive Polarity Reed-Muller (PPRM) S-box. The basic building blocks of S-box are inverter/ buffer, XOR/XNOR and NAND/AND gates. These are implemented with FinFET based ECRL logic, and the S-box is then synthesized. Simulations are carried out with 45 nm FinFET BSIM-CMG model using virtuoso design environment. The performance of ECRL S-box is compared with conventional CMOS S-box over a wide range of supply voltages and frequencies. This paper is structured as follows; section 2 presents the background of adiabatic logic and introduction about FinFET is given in section 3. Section 4 shows the 3-stage PPRM implementation with FinFET. Finally, results and conclusions are given in sections 5 and 6 respectively.

2. Adiabatic Logic

The term adiabatic is a reversible thermodynamic process that occurs without loss or gain of energy. Unlike, the traditional power sources used by conventional CMOS logic circuits, adiabatic logic uses power clock to achieve efficient recycling of the charge stored in load capacitor. This energy recycling minimizes the dynamic switching energy loss. The charging and discharging processes of adiabatic logic are shown in Fig. 1.

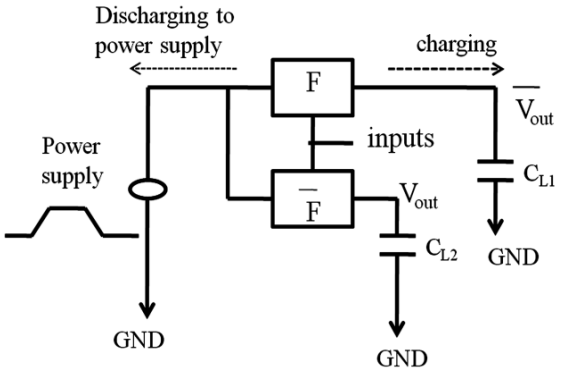


Fig. 1 Adiabatic charging and discharging.

The energy dissipated in an adiabatic circuit when the charge is supplied from a constant current source is given as in Eq. 1. The effective resistance of the driven device is R, and C is the load capacitance.

$$E_{diss} = \frac{RC}{T} CV_{dd}^2 \quad (1)$$

The adiabatic losses show that the speed of operation impacts the energy dissipation as given in Eq. 2.

$$E_{adia} = \frac{R_{on} C}{T} CV_{dd}^2 \quad (2)$$

where R_{on} is on resistance of the device. The non-adiabatic losses are frequency independent, and they are mainly due to variation in threshold voltage, V_{th}. The relation between non-adiabatic energy loss and the threshold voltage is given as in Eq. 3.

$$E_{non-adia} = \frac{1}{2} CV_{th}^2 \quad (3)$$

The leakage losses in adiabatic logic are due to rapid shrinking of transistors and mainly occur during evaluation, hold and recovery. The leakage energy consumption per cycle is given in Eq. 4.

$$E_{leak} = V_{dd} I_{leak} \frac{1}{f} \quad (4)$$

where, I_{leak} is the mean current and f is the power clock frequency. From Eq. 4, it is evident that the leakage energy is inversely proportional to frequency.

Various adiabatic logic families including positive feedback adiabatic logic (PFAL) [13], ECRL [14], clocked adiabatic logic (CAL) [15] and two-phase clocked CMOS adiabatic logic (2PC2AL) [16] are reported in literature. As the security is also one of the to days major consideration, extensive research is available in literature. The circuit complexity in terms of number of devices and power clocks, reliability are the limitations of the secure adiabatic logic families. As there is minimum complexity and power dissipation, ECRL logic is chosen to implement the three-stage PPRM S-box [10]. The ECRL buffer/inverter shown in Fig. 2.

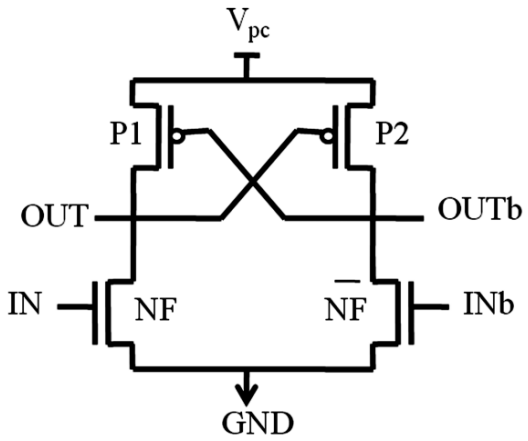
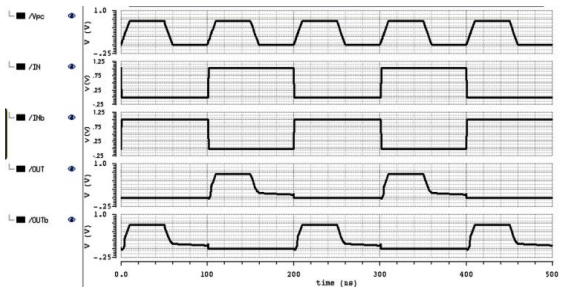
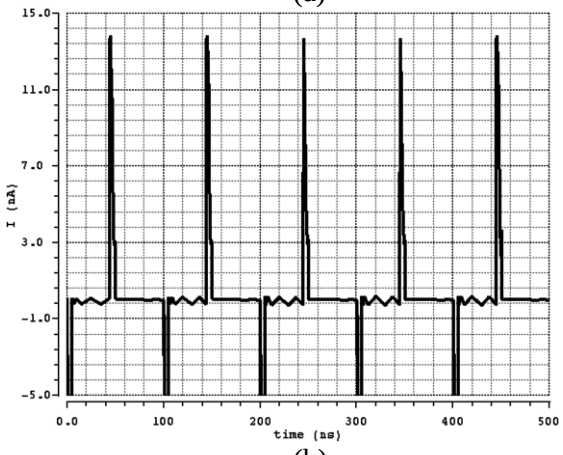


Fig. 2 ECRL buffer/ inverter.

The structure consists of two cross-coupled PMOS devices P1 and P2 to store the information and NMOS devices for implementing the logic. The power supply is V_{pc} and IN, INb, and OUT, OUTb is true and complementary input signals and outputs respectively. The simulated transient response and peak current trace of ECRL buffer/inverter are given in Fig. 3. The current trace shows uniform peak current for '1' to '0' and '0' to '1' transitions.



(a)



(b)

Fig. 3 ECRL buffer/ inverter a) Transient response b) Peak current trace of ECRL buffer/ inverter.

3. FinFET Technology

FinFET consists of a very lean silicon body formed perpendicular to the plane of the wafer and having a three-dimensional structure. The current flows parallel to the wafer plane [13]. Fig. 4 shows the structure of FinFET with the channel is surrounded from three sides by the gate. In this structure W_{fin} is the width of the fin, H_{fin} is fin height, and L_g is gate length. The device can provide powerful control over the channel and suppress the short channel effects (SCEs).Hence FinFET offers lower leakage, higher on-state current and faster-switching speed. The leakage current is found to be of the order of Pico amperes. The multi-gate nature allows FinFET to be operated in three different modes, namely, independent gate (IG), shorted gate (SG) and low-power (LP) modes.

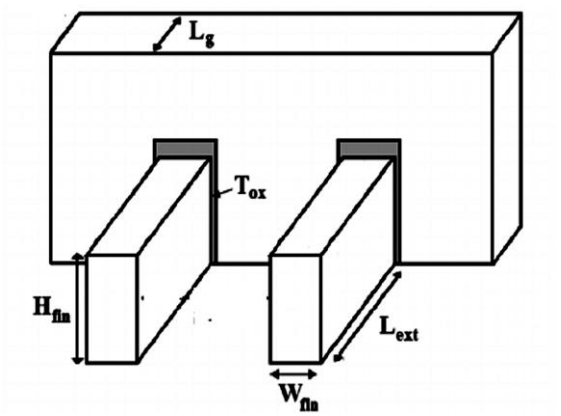


Fig. 4 Structure of FinFET.

4. PPRM S-Box

Cryptography is an essential tool for protecting information in computer systems. National institute of standards and technology (NIST) selected advanced encryption standard (AES) based on Rijndael algorithm [14] as data encryption standard according to the primary criteria of security, performance, and efficiency. AES is one of the widely used algorithms for different applications like wireless sensor networks (WSN) and IoT. The efficiency of AES hardware depends on its architecture [15]. The AES implementation is shown in Fig. 5.

In general, there are two methods for S-box circuit implementation, (i) construction of multiplicative inverse and affine transform in an independent manner and connecting

them serially, which reduces area with composite field arithmetic [16] and (ii) construction of a single circuit. In this technique, S-box is implemented from truth table itself as the sum of products (SoP), a product of sums (PoS), and PPRM [17]. Among these two techniques, the PPRM S-box consumes more power compared to composite field S-box due to a large number of signal transition probabilities. This problem can be avoided by taking three sub-components of composite field S-box and convert them to PPRM form, namely, the pre-inversion, inversion and post-inversion sections as depicted in Fig. 6. Each section when implemented with two-level AND and XOR arrays reduces the signal transition probability, thus leading to efficient utilization of power [18-19]. PPRM form, also called the zero polarity form is a XOR sum of products where each variable is in un-complemented form. Any n-variable logic function is represented in PPRM form as given in Eq. 5.

$$f(x_{n-1}x_{n-2}.....x_0) = b_0 \oplus b_1 x_0 \oplus b_2 x_1 \oplus ... \oplus b_{2^n-1} x_{n-1} x_{n-2} .... x_0 \quad (5)$$

In this x_0 - x_{n-1} are Boolean variables and b0 - b_{2^n-1} are the corresponding coefficients.

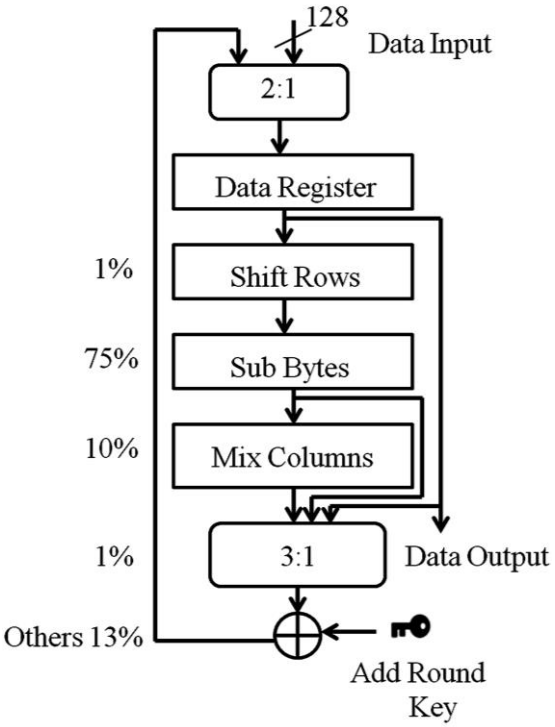


Fig. 5 Standard implementation of AES and power consumption of each block.

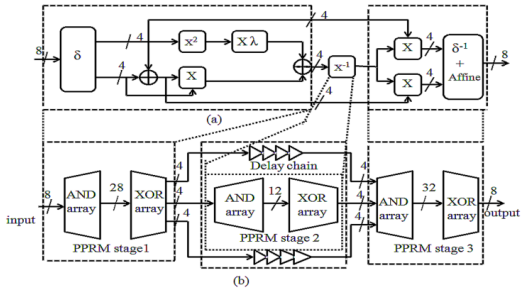


Fig. 6 Mapping of composite field S-box to three-stage PPRM S-box a) Composite field b) PPRM.

The two-input ECRL AND/NAND, XOR/XNOR gates using FinFET is shown in Fig. 7. The front gate of the FinFET is used as input, while the back gate of P FinFET is connected to V_{pc} and N FinFET to ground for low power operation. With the structure of conventional XOR gate, the transition probability of the output depends largely upon the input. In-order to reduce this dependency, a control signal 'S' is used. In this X and Y are dual inputs and OUT and OUTb are the outputs with V_{pc} as four-phase power clock supply.

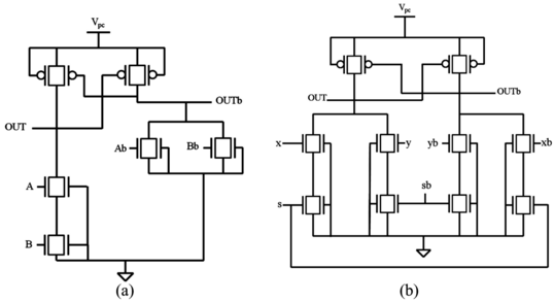
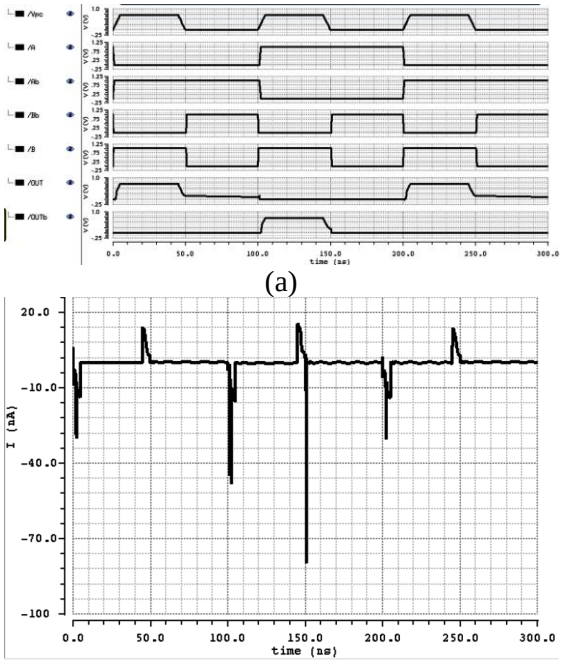


Fig. 7 Two-input ECRL a) AND/NAND gate b) XOR/XNOR gate using FinFET.

The simulated transient response and peak current trace of ECRL AND/NAND gate is shown in Fig. 8. The circuit has dual inputs A, B and outputs OUT and OUTb. The current trace plot of the circuit shows same peak value of current and also exhibits uniform low-power dissipation for different input transitions.

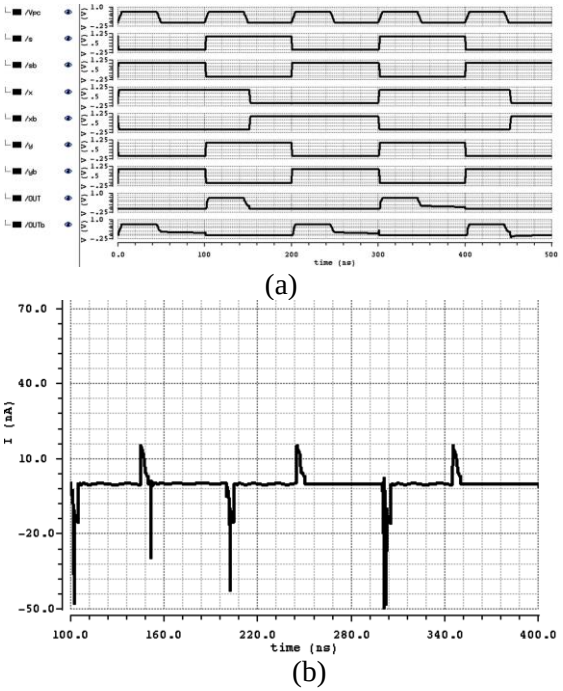


(a)

(b)

Fig. 8 ECRL AND/NANG gate a) Transient response b) Peak current trace.

The simulated transient analysis and the peak current trace of XOR/XNOR gate is depicted in Fig.9. The structure given will ensure a uniform peak current for the input transitions. Thus there is less probability for the hacker to predict the input data in cyber security hardware.



(a)

(b)

Fig. 9 ECRL XOR/XNOR gate a) Transient response b) Peak current trace.

5. Results and Discussion

Simulations are carried out on both CMOS and FinFET based ECRL 8-bit S-box circuits using 45nm BSIM-CMG model. The device parameters chosen for CMOS are L=45nm, W=90nm, and V_{th}=0.6V, while for FinFET, L=45nm, T_{fin}=15nm, H_{fin}=30nm, T_{ox}=1nm and V_{th}= 0.4V. The width of the FinFET device is obtained from the following relation.

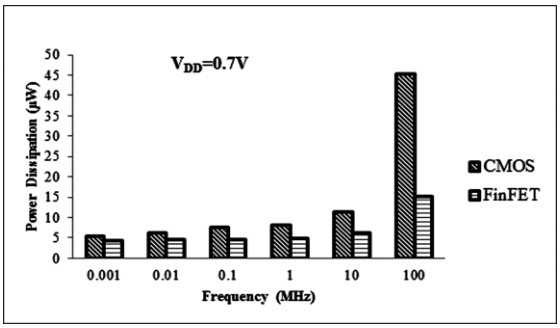
$$W_{fin} = 2H_{fin} + T_{fin} \quad (6)$$

The supply voltage is varied from 0.5 to 1V and the input power clock frequency from 0.001 to 100 MHz. Table 1 gives a comparison of the area between CMOS and ECRL FinFET implementations. The results indicate an area reduction of 11.6% with ECRL FinFET circuit.

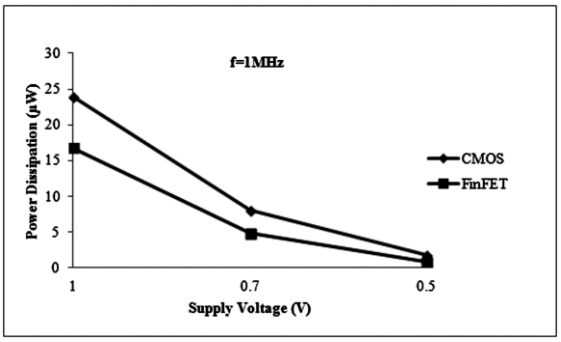
Table 1 Area comparison of CMOS and FinFET based ECRL S-box.

No. of devices	CMOS	FinFET
PMOS transistors	1842	798
NMOS transistors	1842	2458
Area (nm^2)	0.0149	0.0138

Fig. 10 shows the histogram of average power dissipation with frequency and effect of supply voltage scaling on power dissipation. Power savings of the order of 22-66% are achieved with FinFET relative to CMOS over a frequency band of 0.001 to 100 MHz.



(a)



(b)

Fig. 10 PPRM S-box a) Power dissipation with power clock frequency, b) Supply voltage scaling effect on power dissipation.

The S-box is simulated at a 12.5 MHz frequency to demonstrate its usage in contact-less smart card applications. Table 2 shows the comparison of power dissipation, delay, and energy dissipation over a cycle at 12.5 MHz, and V_{pc} of 0.7V. The power dissipation and delay results of the present study are compared in table 3 with different technology nodes at 10 MHz frequency.

Table 2 Comparison of S-box performance parameters.

Parameter	CMOS	FinFET
Power dissipation (µW)	11.28	5.91
Delay (nS)	1.19	2.5
Energy dissipation (fJ)	1024	726.3

Table 3 Power dissipation and delay comparison of 8-bit S-box circuit for different technology nodes at 10 MHz frequency.

Reference	Technology node	Power dissipation (µW)	Delay (nS)
[17]	180nm (MOSFET)	51	1.86
[18]	180nm (MOSFET)	28	-
This work	45nm (FinFET)	6.06	2.5

Further, to validate our design to DPA attacks, statistical analysis of normalized energy deviation (NED) and normalized standard deviation (NSD) are carried out by measuring energy dissipation as follows.

$$E_{diss} = \int_0^T V_{pc}(t) I_{pc}(t) \tag{7}$$

where I_{pc} is the supply current, NED and NSD determine the ability of the design against power analysis attacks depending upon the input transitions.

$$NED = \frac{\left(E_{\max} - E_{\min}\right)}{E_{\max}} \tag{8}$$

$$NSD = \frac{\sigma_E}{\overline{E}} \tag{9}$$

where $\overline{E}$ is the average energy dissipation and is given in Eq. 10.

$$\overline{E} = \left(\sum_{i=E_1}^{E_n} E_i\right) \Big/ n \tag{10}$$

The standard deviation is defined as in Eq. 11.

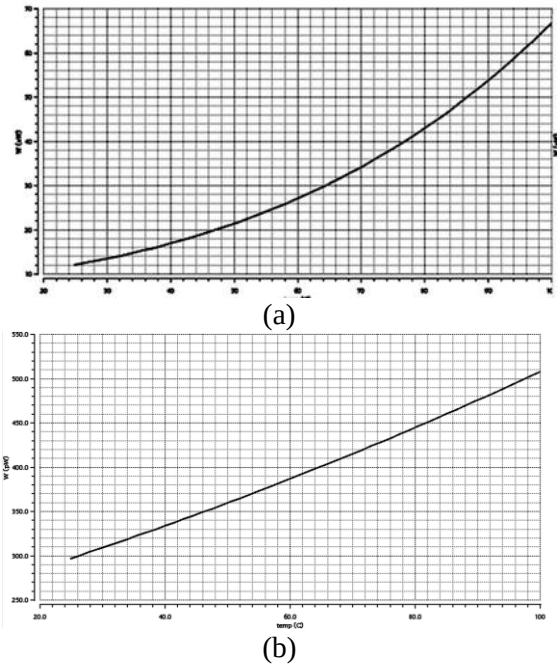
$$\sigma_E = \sqrt{\sum_{i=E_1}^{E_n} \left(E_i - \overline{E}\right)^2 \Big/ n} \tag{11}$$

E_{max}, E_{min}, and n are the maximum energy, minimum energy, and number of energy samples respectively. 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. From the results of the ECRL FinFET 8-bit S-box circuit summarised in table 4 it is observed that in the medium frequency range, up to about 50MHz, the designed S-box is more resistant to DPA attacks. Table 4shows the calculated values of NED and NSD of designed S-box circuit.

Table 4 Simulation and calculated values of energy of ECRL FinFET 8-bit S-box circuit for different input power clock frequencies

Frequency (MHz)	1	10	12.5	50	100
$E_{min\ (pJ)}$	8.76	9.75	15.23	25.41	32.40
$E_{max\ (pJ)}$	9.15	10.77	17.30	29.93	40.28
$\overline{E}_{(pJ)}$	9.04	10.02	18.80	28.66	36.50
NED (%)	8.18	9.47	12.13	15.13	19.56
NSD (%)	13.8	10.2	11.4	14.06	34.3

To assess the designed S-box circuit reliability with temperature, the change in power dissipation with temperature is analysed over the range of 20-100^{0}C is shown in Fig. 11. The power dissipation trend for a CMOS based S-box is exponential in nature, and it is found to be of the order of nW, whereas, for FinFET circuit the power dissipation exhibits a linear relationship with increase in temperature and is in the range of pW.



(a)

(b)

Fig. 11 Effect of temperature on power dissipation of ECRL S-Box a) CMOS and b) FinFET circuit.

6. Conclusion

In this work, various design possibilities are explored to minimize the power consumption of S-box circuit. To achieve the design target, a three-stage PPRM based S-box is implemented with CMOS and FinFET based ECRL logic. Various performance parameters such as power dissipation, area are measured with supply voltage scaling and input frequency. Results indicate an improvement in power savings of the order of 22-66% in 0.001-100 MHz frequency range for the FinFET based ECRL logic over CMOS circuit. Further, the designed S-box consumes uniform transitional energy dissipation up to about 50 MHz, and exhibits similar peak supply current trace which improves the resistant to DPA attacks, thus making it suitable for low-power and secures devices in low-frequency bands, such as RFID tags, contact-less smart cards, IoT and wireless sensors.

References

[1] National Institute of Standards and Technologies (2001) Announcing the Advanced Encryption Standard (AES). *Federal Information Processing Standards Publication*. no. 197.

[2] Yong Bin Zhou, Deng Guo Feng (2005) Side-Channel Attacks: Ten Years after Its Publication and the Impacts on Cryptographic Module Security Testing. *IACR Cryptology* ePrint Archive. pp. 1-34.

[3] Paul Kocher, Joshua Jaffe, and Benjamin Jun (1999) Differential Power Analysis, Advances in Cryptology, *LNCS*, Vol. 1666, pp. 388–397.

[4] 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.

[5] Amir Moradi and Axel Poschmann (2010) Light Weight Cryptography and DPA Countermeasures: a Survey, Proc. *Int. Conf. on Financial Cryptography and Data Security*, pp. 68-79.

[6] Athas W. C., L. J. Sevensson, J. G. Koller, N. Tzartzains, and E. Y. C. Chou (1994) Low-Power Digital Systems Based on Adiabatic Switching Principles, *IEEE Trans. Very Large Scale Integr. Syst*., Vol. 2, No. 4, pp. 398-407.

[7] Mukhopadhyay S., A. Raychowdary, and K. Roy (2005) Accurate Estimation of

Total Leakage in Nanometer-Scale Bulk CMOS Circuits Based on Device Geometry and Doping Profile, *IEEE Trans. Comput.-Aided Design Integr. Circuits and Syst*., Vol. 24, No.3, pp. 363-381.

[8] 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 Self-Aligned Double Gate MOSFET Scalable to 20nm, *IEEE Trans. Electron Device*s, Vol.47, No.12, pp. 2320–2325.

[9] Dressen D. (2004) Considerations for RFID Technology Selection, *Atmel Applications Journa*l, Vol. 3, pp. 45-47.

[10] Srilakshmi K., A. V. N. Tilak, and K. Srinivasa Rao (2016) Performance of FinFET Based Adiabatic Logic Circuits, *Proc. of IEEE Int. Conf*. (TENCON-2016), pp. 2379-2384.

[11] Alioto M., S. Bongiovanni, M. Djukanovic, G. Scotti, and A. Trifiletti (2014) Effectiveness of Leakage Power Analysis Attacks on DPA-Resistant Logic Styles Under Process Variations, *IEEE Trans. Circuits Syst. I Reg. Papers*, Vol. 61, No.2, pp. 429-442.

[12] Teichmann P. (2012) Adiabatic Logic: Future Trend and System Level Perspective, Springer, Vol. 34, Edition 1, pp. 5-22.

[13] Katrine Lundager, Behzad Zeinali, Mohammad Tohidi, Jens K. Madsen, and Farshad Moradi (2016) Low Power Design for Future Wearable and Implantable Devices, *J. Low Power Electronics and Applications*, Vol. 2, No. 26, pp. 1-26.

[14] Daemen J. and V. Rijmen (2002) The Design of Rijindael-AES-The Advanced Encryption Standard, Springer Verlag.

[15] Gaj K. and P. Chodowiec (2008), FPGA and ASIC implementation of AES, Cryptographic Engineering, Springer, pp. 235-294.

[16] Menezes A.J., I.F. Blake, X. Gao, R.C. Mullin, S.A. Vanstone, and T. Yaghoobian (1993) Applications of Finite Fields, Springer Intl. Series.

[17] Sasao T. (1993) AND-EXOR Expressions and their Optimization, Logic Synthesis and Optimization, Kluwer Academic Publishers, pp. 287–312.

[18] 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.

[19] Cancio Monteiro, Yasuhiro Takahashi, and Toshikazu Sekine (2013) Low Power Secure AES S-box using Adiabatic Logic Circuit", *Proc. of Faible Tension Faible Consommation* (FTFC), pp. 1-4.