DOI: 10.21917/ijme.2020.0168

ULTRA LOW POWER AND SECURE VLSI ARCHITECTURE FOR DEDICATED SHORT RANGE COMMUNICATION APPLICATIONS

Radha Kollipara[1] and Venkata Nagaratna Tilak Alapati[2]

[1]*Department of Electronics and Communication Engineering, Sir C.R. Reddy College of Engineering, India*

[2]*Department of Electronics and Communication Engineering, Gudlavalleru Engineering College, India*

Abstract

Dedicated Short Range Communication (DSRC) is being widely deployed in intelligent transportation systems. The DSRC standards typically choose to take up line codes such as Manchester, differential Manchester, and FM_0 codes to achieve dc balance. In this paper, low power and secure VLSI architecture for integrated codes is proposed. The performance of the circuit is evaluated using 18nm FinFET based ECRL adiabatic logic in Cadence tool. The average power dissipation of multimode encoder operating at 877.192MHz is observed to be 32.24 µw. The design provides not only 100% hardware utilization rate (HUR) but also maximum power saving of 99.99% over reported values for FPGA implementation. The adiabatic logic circuits designed with ECRL exhibit uniform peak current traces and hence are able to withstand differential power analysis (DPA) attacks, thereby offering improved security performance of the circuit.

Keywords:

DSRC, Encoder, Adiabatic, DPA, FinFET

1. INTRODUCTION

The autonomous vehicle technology is gaining importance now-a-days. These vehicles analyze their surroundings with the help of sensors and cameras. The visual information from these devices has limitations in providing safety to the vehicle users. Better traffic management is essential in saving people from road and highway accidents. The dedicated short range communication (DSRC) [1], [2] is useful for a one or two-way medium range transmission between vehicles, vehicle to road side infrastructure, and vehicle to everything. It enables sending of messages and broadcasting these messages among vehicles for announcement of public information and safety issues [3], [4]. To avoid collisions, inter and intra-vehicular communication is considered very crucial in terms of reliability, accuracy and confidentiality [5]. DSRC, with broader perspective of its surroundings by understanding road and traffic that are not easily visible to cameras, can reduce the risks of collisions and accidents.

The DSRC system consists of a transceiver and transponders. The semi-passive transponders operate with the help of batteries. They retransmit the same signal sent by the transceiver and perform frequency shift and encoding of information to be transmitted. Despite advancements in low-power integrated circuits technology, the life of the battery is limited. A totally independent DSRC transponder is not viable in terms of energy consumption. In order to extend the life of the battery, it is required to design DSRC transponder with reduced power consumption.

The remaining part of the paper is organized as follows. Literature review is carried out in section 2 and brief description about adiabatic logic and FinFET device is given in section 3. In section 4, the architecture of multimode encoder is described. The results are given in section 5 and lastly section 6 concludes the paper.

2. LITERATURE REVIEW

In automotive electronic systems, security plays a crucial role. In these systems, vehicles may prone to attacks from various interfaces such as direct / indirect physical access, short range and long range wireless communication access channels. Hence, it is necessary to provide security in DSRC communications as the basic safety messages (BSM) convey significant information for safety [6]. An attacker can access different electronic control units (ECUs) and safety related critical components. The ECU provides different security applications such as forward collision warning, left turn assistance and lane change warning, etc. In addition, other performance metrics in DSRC system such as energy efficiency, safety, and congestion control are evaluated.

DSRC is the basic platform for many applications of automotive systems. DSRC standard requires encoding of the information bits to increase signal reliability and to provide dc balance [7], [8]. The problem of dc balancing can be overcome by using different encoding mechanisms that the DSRC supports are Manchester, differential Manchester [9] and FM_0. The design and development of multimode encoder suitable for DSRC using CMOS technology, though offers low power dissipation, it suffers from differential power analysis (DPA) attacks, causing security problems. Also, with the scaling of technology, leakage power increases. In the proposed work, to reduce the leakage power and to provide security to DSRC system, FinFET based adiabatic logic is used for the design of multimode encoder. One of the most commonly used adiabatic logic is efficient charge recovery logic (ECRL). The circuits designed with ECRL are found to have constant current peaks, thus offering resistance to DPA attacks [10]. The FinFET design [11] offers low leakage power and that in combination with adiabatic logic [12] which recycles the consumed energy, provides energy efficiency for the circuit. Simulations are carried out with 18 nm FinFET NMOS/PMOS standard threshold voltage (SVT) cells using Cadence tool.

3. BACKGROUND

3.1 DSRC

The architecture of DSRC system is shown in Fig.1. It mainly consists of microprocessor, baseband processing, and radio frequency (RF) units. The microprocessor interprets the media access control instructions to schedule the baseband processing tasks and radio frequency front-end. The baseband process unit is liable for modulation, error correction, clock synchronization, and

encoding. The transmission and reception of wireless signal is achieved by the RF frontend through the antenna.

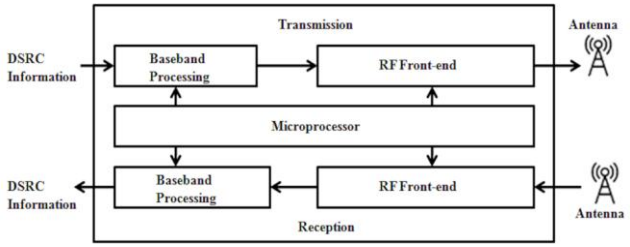


Fig.1. Architecture of DSRC system

3.2 ADIABATIC LOGIC

In conventional CMOS circuits, an energy of $0.5CV^{2}_{DD}$ is stored in the output node capacitance C during charging from the constant supply voltage V_{DD}. This energy is released during discharge of C and therefore no energy can be recovered.

For minimization of energy loss at all circuit nodes during charging and discharging periods, adiabatic switching is widely used [13]. The energy dissipated is given as

$$E_{diss} = 2CV^{2}_{DD}\,(RC/\tau) \quad (1)$$

where R is the effective resistance, C is the output node capacitance, τ is the switching time, and V_{DD} is the voltage to be switched across. When τ is very large, the energy Ediss tends to be zero ideally.

3.3 FINFET DEVICE

In CMOS circuits, the leakage power is increased by the aggressive scaling of technology and threshold voltage of the device. FinFET, a quasi-planar double-gate device is found to be a good alternative for addressing the challenges due to scaling and to lower the leakage power.

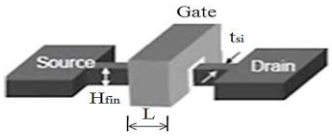


Fig.2. Structure of FinFET

The Fig.2 shows the structure of FinFET with fin height (Hf_{in}) and silicon thickness (t_{si}). This device significantly reduces the leakage power by suppressing the gate-dielectric leakage current and short-channel effects (SCEs). With independent control of its gates [14] the FinFET device also offers design flexibility.

3.4 EFFICIENT CHARGE RECOVERY LOGIC (ECRL)

Over the last few years, several adiabatic logic families, like efficient charge recovery logic (ECRL) [15], [16], clocked adiabatic logic (CAL), positive feedback adiabatic logic (PFAL), etc. are reported in the literature. The symmetric structure of ECRL [17] logic helps in attaining data independent power consumption. For this, equal number of transistors at the both normal and complementary output nodes for each input transitions are turned ON. In this case, the two output nodes of the ECRL gate charge equal amount of capacitance. Thus, by making its discharge circuit as symmetric, the ECRL circuit can be effective against differential power analysis (DPA) attacks [17], [18]. The ECRL based buffer/inverter, NAND/AND, XNOR/ XOR, and multiplexer are shown in Fig.3.

The ECRL buffer/inverter [19] shown in Fig.3(a) comprises two cross-coupled PMOS devices P_1 and P_2 in the pull-up network to store the information. The logic is implemented by the NMOS devices in the pull-down network. In the Fig.3(a) shown, pclk is the power supply, *in*, in_b and *out*, out_b are the true and complementary input and output signals respectively.

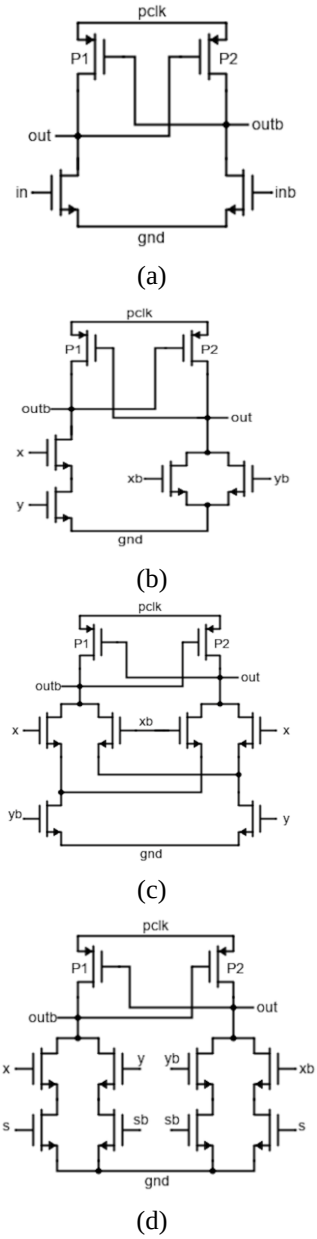


Fig.3. ECRL based (a) buffer/inverter, (b) NAND/AND gate, (c) XNOR/XOR gate, and (d) multiplexer

The logic diagram of a positive edge-triggered D flip-flop is given in Fig.4. It consists of asynchronous inputs preset and clear. The output Q of the flip-flop depends only on the input D and its state changes at the positive edge of the clock whenever asynchronous inputs are not activated.

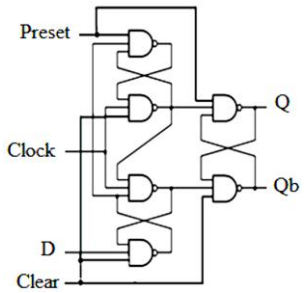


Fig.4. Positive edge-triggered D flip-flop

4. MULTIMODE ENCODER ARCHITECTURE

The structure of FM_0 code is shown in Fig.5. For each bit of input data *D*, the FM_0 encoded output comprises of first half-cycle of the clock *Y* and the second half-cycle of the clock *Z*. The principles of FM_0 coding are

- If *D* is logic 0, a transition takes place between *Y* and *Z* in the FM_0 code.
- No transition takes place between *Y* and *Z* if *D* is logic 1.
- A transition occurs among every FM_0 code irrespective of the status of *D*.

An example of FM_0 coding is given in Fig.6. When *D* is logic 0 at cycle one, there occurs a transition as per rule 1. For convenience, at first, this transition is considered to occur from 0 to 1. A transition takes place between every FM_0 code according to rule 3. Hence the logic 1 undergoes a change of logic 0 at the start of cycle 2. As per rule 2, this logic level remains constant with no transition takes place throughout the cycle 2 when *D* is logic1.

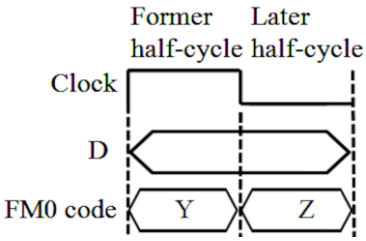


Fig.5. Structure of FM_0 code

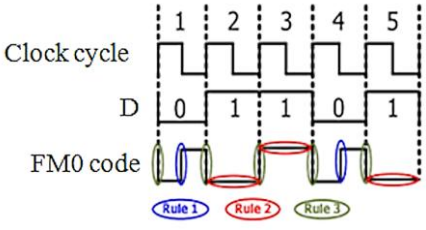


Fig.6. Example of FM_0 coding

The Fig.7 illustrates Manchester encoding. An XOR operation for clock and *D* results in Manchester code. Here also there is a transition in the clock cycle independent of *D* value.

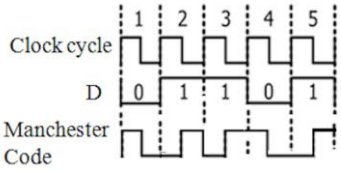


Fig.7. Example of Manchester coding

In differential Manchester (DM) encoding, the presence or absence of transitions indicates the logic value. There is no need to know about the sent signal polarity, as the information is present in their changes and not in the voltage levels. This makes the synchronization easier. The Fig.8 shows the example of differential Manchester coding.

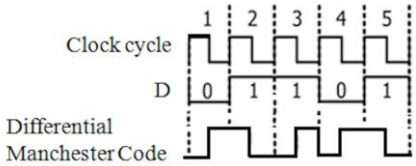


Fig.8. Example of differential Manchester coding

The proposed multimode encoder architecture is shown in Fig.9. The switching between three codes is achieved by means of different combinations of the mode signals M_1, M_2, and the clear signal CLR It makes use of a positive edge-triggered *D* flip-flop.

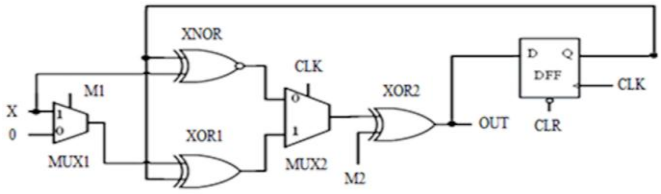


Fig.9. Multimode encoder architecture

When M_1=1, M_2=1, *CLR*=0 then the architecture works as Manchester encoder, when M_1=0, M_2=1, *CLR*=1 then it works as FM_0 encoder. The differential Manchester encoder operation occurs when M_1=1, M_2=1, *CLR*=1.

5. RESULTS AND DISCUSSION

The simulation results for the Manchester encoder operating at a maximum frequency of 877.192MHz with capacitance CL=20fF and with a 32-bit input pattern as, 01001011111000110 100101111100011 are shown in Fig.10. An XOR operation for clock and 32-bit input data results in Manchester code. A transition occurs in every clock cycle, independent of the input data. Low to high level and high to low level changes occur for bit ‘1’and bit ‘0’ respectively. In the 32-bit pattern shown in Fig.10, as the first bit is ‘0’, high to low level transition is observed, and for the next bit ‘1’, the transition is from low to high, and so on.

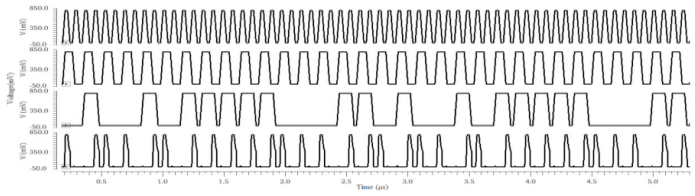


Fig.10. Simulation results of Manchester encoder for the 32-bit pattern 01001011111000110100101111100011

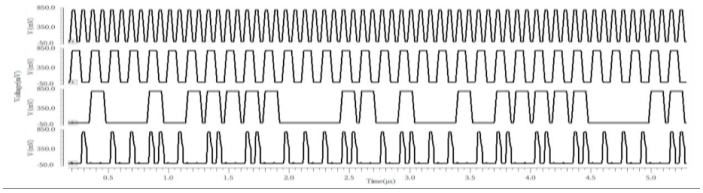


Fig.11. Simulation results of FM_0 encoder for the 32-bit pattern 01001011111000110100101111100011

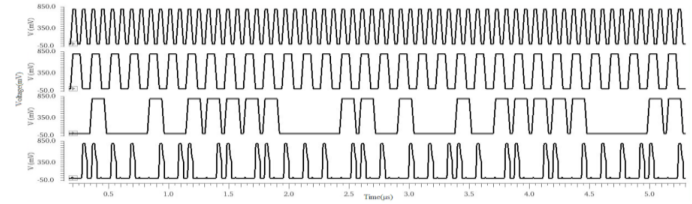
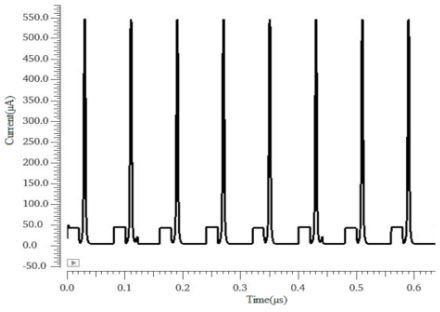
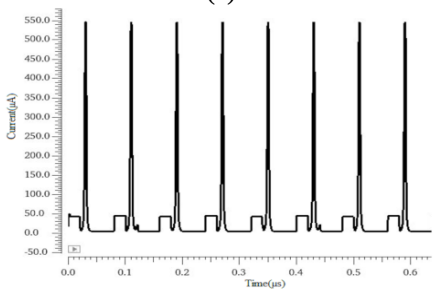


Fig.12. Simulation results of differential Manchester encoder for the 32-bit pattern 01001011111000110100101111100011

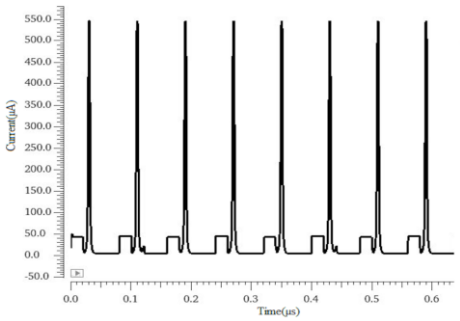
The Fig.11 and Fig.12 give the simulation results for the 32-bit input FM_0 and differential Manchester encoders respectively.



(a)



(b)



(c)

Fig.13. Peak current traces of multimode encoder operating in three modes (a) Manchester mode, (b) FM_0 mode, and (c) differential Manchester mode

In FM_0, for bit '1' there will be no mid bit transition. For bit '0', there will be a mid-bit transition either from low to high level or vice versa. Also, a transition occurs among every FM_0 code irrespective of the status of the input bit. It can be noted from Fig.11 that the first bit is '0' causes a transition from low to high and no transition occurs in the total cycle as the subsequent bit is '1'.

In case of differential Manchester encoder for bit '1' or '0', mid bit transition will be either from low to high level or vice versa. A transition occurs toward the beginning of the bit span for input bit 0 and no change for input bit 1. It can be observed from Fig.12 that as the first bit is '0', mid bit transition occurs. Since the second bit is '1', no transition occurs at the start of the bit interval, but mid bit transition takes place.

Though the multimode encoder can be designed by using the CMOS technology, they are prone to differential power analysis (DPA) attacks because of higher leakage power. To eliminate DPA attacks, adiabatic technique has been proposed. A supply current that is independent of input data in the ECRL adiabatic logic was verified by Cadence Virtuoso simulations. The peak current traces of multimode encoder operating in three modes are given in Fig.13. The uniform peak current traces in these figures indicate resistance to differential power analysis attacks, thus protecting the data from unauthorized access and providing security.

Table.1. Effect of supply voltage scaling on power dissipation.

Supply Voltage (V)	Average Power (µw)
1.0	442
0.9	76.14
0.8	32.24
0.7	18.76
0.6	9.9
0.5	5.25

The effect of supply voltage scaling on power dissipation for multimode encoder operating in three modes is given in Table.1. The power dissipation is observed to be reduced by 98.81% as the supply voltage is scaled from 1 to 0.5V.

Simulations are carried out on FinFET based ECRL multimode encoder circuit using NMOS/PMOS SVT cells. A trapezoidal signal acts as a power clock with a peak voltage of

0.8V and a frequency of 12.5MHz. Every logic block of the multimode encoder architecture is made use of in all the three encoding schemes specified, giving rise to 100% hardware utilization rate (HUR). The Table.2 presents the comparison of performance characteristics of adiabatic multimode encoder with the reported values [20].

Table.2. Comparison of performance characteristics of adiabatic multimode encoder with reported values.

Parameter	[20]	This work
Realization	Xilinx Virtex 5 FPGA	18nm FinFET
Supply voltage	-	0.8V
Coding methods	Manchester, FM_0, Differential Manchester	Manchester, FM_0, Differential Manchester
Operating frequency	433 MHz	877.192MHz
Power consumption	34 mw	32.24µw
Delay	-	5.7ns
Energy	-	183.77fJ
HUR (Components Active / Total)	100%	100%

Power savings of the order of 99.99% are achieved with adiabatic logic implementation for all the three encoders.

6. CONCLUSION

DPA attacks have become a serious threat to various DSRC devices. Adiabatic logic is considered as a possible solution to design DPA countermeasure circuit which consumes ultra-low power as compared to the other circuit level CMOS circuits. Among various adiabatic logic families, ECRL is found to be very attractive for low-power applications. To make the ECRL adiabatic logic independent of the input data, the discharge circuit is made as symmetric. In this work, a multimode encoder is implemented with FinFET based ECRL adiabatic logic. From the results it is observed that there is an improvement in power savings of the order of 99.99% over FPGA based implementation. Further, the designed multimode encoder exhibits consistent peak supply current traces indicating improved resistance to DPA attacks. Thus the ECRL based multimode encoder can be very attractive for power sensitive encryption device. Further, this multimode encoder architecture achieves 100% hardware utilization rate. In order to ensure an error-free DSRC communication system along with security and power efficient encoder design, error control mechanism can be adopted.

REFERENCES

[1] F. Ahmed Zaid, F. Bai and S. Bai, "Vehicle Safety Communications Applications (VSC-A) Final Report", Available at: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/811492a.pdf.

[2] Wu Xinzhou, Subramanian Sundar and Guha Ratul, "Vehicular Communications using DSRC: Challenges, Enhancements, and Evolution", *IEEE Journal on Selected Areas in Communications*, Vol. 31, No. 9, pp. 399-408, 2013.

[3] J.B. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the United States", *Proceedings of the IEEE*, Vol. 99, No. 7, pp. 1162-1182, 2011.

[4] D. Jiang, V. Taliwal and A. Meier, "Design of 5.9 GHz DSRC based vehicular safety communication", *IEEE Wireless Communications*, Vol. 13, No. 5, pp. 36-43, 2006.

[5] C. Laurendeau and M. Barbeau, "Threats to security in DSRC/WAVE", *Proceedings of 5th International Conference on Ad-Hoc Networks and Wireless*, pp. 266-279, 2006.

[6] Chung Wei Lin and Alberto Sangiovanni Vincentelli, "*Security-Aware Design for Cyber-Physical Systems: A Platform-Based Approach*", 1st Edition, Springer Publisher, *2017.*

[7] Y. Lee and C. Pan, "Fully Reused VLSI Architecture of FM0/Manchester Encoding using the SOLS Technique for DSRC Applications", *IEEE Transactions on Very Large-Scale Integration (VLSI) Systems*, Vol. 23, No. 1, pp. 18-29, 2015.

[8] Y. Lee, C. Pan and F. Tsai, "VLSI Architecture design of FM0/Manchester Codec with 100% Hardware Utilization Rate for DSRC based Sensor Nodes in its Applications", *IEEE Sensors Journal*, Vol. 15, No. 12, pp. 6875-6889, 2015.

[9] G. Siva Jyothirmai and T. Sudheer Kumar, "On the Implementation of VLSI Architecture of FM0/Manchester Encoding and Differential Manchester Coding for Short-Range Communications". *Proceedings of International Conference on Microelectronics, Electromagnetics and Telecommunication*, pp. 551-558, 2018.

[10] D. Wu, X. Cui and W. Wei, "Research on Circuit Level Counter Measures for Differential Power Analysis Attacks", *Proceedings of International Conference on Solid State and Integrated Circuit Technology*, pp. 1-3, 2012.

[11] A.N. Bhoj and N.K. Jha, "Design of Logic Gates and Flip-Flops in High Performance FinFET Technology", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol.* 21, No. 11, pp. 1975-1988, *2013.*

[12] P. Teichmann, "*Adiabatic Logic*", Springer Publisher, 2012.

[13] Kaza Srilakshmi, A.V.N Tilak and Karumuri Srinivasa Rao, "Ultralow-Power, and Secure S-Box Circuit using FinFET Based ECRL Adiabatic Logic", *Journal of Science and Technology*, Vol. 10, No. 3, pp. 10-17, 2018.

[14] P. Mishra, A. Muttreja and Niraj K. Jha., "*FinFET Circuit Design*", Springer, 2011.

[15] M.Sanadhya and M.V. Kumar, "Recent Developments in Efficient Adiabatic Logic Circuits and Power Analysis with CMOS Logic", *Procedia Computer Science*, Vol. 57, pp. 1299-1307, 2015.

[16] Y. Moon and D.K. Jeong, "An Efficient Charge Recovery Logic Circuit", *IEEE Journal of Solid-State Circuits*, Vol. 31, No. 4, pp. 514-522, 1996.

[17] H. Thapliyal, T.S.S. Varun and S.D. Kumar, "Adiabatic Computing based Low Power and DPA-Resistant Lightweight Cryptography for IoT Devices", *Proceedings of International Conference on VLSI*, pp. 621-626, 2017.

[18] S.D. Kumar, H. Thapliyal and A. Mohammad, "FinSAL: A Novel FinFET based Secure Adiabatic Logic for Energy-Efficient and DPA Resistant IoT Devices", *Proceedings of International Conference on Rebooting Computing*, pp. 1-8, 2016.

[19] Akash Mondal, Anirban Chowdhury and Sandipta Mal., "Analysis of Adiabatic ECRL NAND/NOR for Ultra Low Power Near-Threshold Computing", *Proceedings of International Conference on Devices for Integrated Circuit*, pp. 456-461, 2017.

[20] P. Ishwerya, V. Nithish Kumar, and G Lakshminarayanan, "An Efficient Digital Baseband Encoder for Short-Range Wireless Communication Applications", *Proceedings of International Conference on Electrical, Electronics, and Optimization Techniques*, pp. 2775-2779, 2016.