International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST

# Implementation of High-Speed Approximate Adiabatic Logic Using Lector Approach for Security Enhancement

**Vikram Dhoni[1], Vilaskumar Patil[2]. Veeresh Kumasigi[3]**
[1]M.Tech. Student, Department of ECE (VLSI & EMBEDDED SYSTEM), Sharnbasva University, Kalaburgi, India
[2]Associate Professor, Department of ECE, Sharnbasva University, Kalaburgi, India
[3]Assistant Proffesor, Department of ECE, VNEC, Shorapur, India.

**Article Info**
Volume 9, Issue 4
Page Number : 353-360

**Publication Issue**
July-August 2022

**Article History**
Accepted : 10 July 2022
Published : 26 July 2022

## ABSTRACT

On Internet of Things edge devices, approximation computing is used in error-tolerant applications is a viable choice for reducing power usage. Assaults via side channels, Differential power analysis, for example, is a distinct story, but it can be used to sabotage approximation calculation (DPA). The use of adiabatic logic in estimation edge computing could help to reduce energy consumption while simultaneously increasing security against side-channel attacks. Despite the fact that approximation and adiabatic logic-based solutions save space and improve security, they consume more power and take longer to complete. To reduce overall size the recommended approximation adders take advantage of adiabatic logic's dual-rail functionality to reduce both the use of electricity and the use of energy are two different things. The article starts with a proposed designs TSAA then moves on to a 2nd proposed design of TCAA.TSAA and TCAA based on adiabatic logic require fewer transistors than a CMOS-based accurate mirror adder. With a 45 nm technology node and a particular operational frequency, the adiabatic design of both proposed 1st & 2nd demonstrated significant power and energy savings over the conventional CMOS AMA. Both proposed architectures are also more resistant to DPA assaults, as demonstrated.

**Keywords :** DPA (Differential Power Analysis), AMA, TSAA, TCAA.

## I. INTRODUCTION

The rise of IoT edge computing [1], [2], which places processing at the network's edge, necessitates more energy-efficient and secure solutions. Adiabatic logic and approximation computation are two new techniques for creating low-power circuits. Accuracy is a trade-off in approximate computing to save space. It appears to be promising for IoT edge device error-tolerant programs.

Cyber security solutions, on the other hand, have not yet been adequately addressed [3, 4]. According to [3,]

an approximation the adder's output and power consumption have a positive relationship that increases as the mistake rate increases. Non-approximation circuits, such as cryptography, run at lower frequencies and supply voltages than approximate circuits, making reverse engineering easier [4]. In order to attack the approximation circuits, adversaries could employ techniques like as well as reverse engineering and side-channel attack.

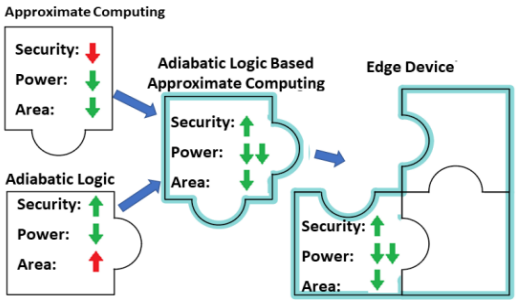


Fig1: By combining adiabatic logic and approximation computation

The load capacitor's energy can be reused by reusing it, adiabatic logic enables for more energy-efficient computing.

The majority of adiabatic logic families have two rails. As a result, in comparison to regular CMOS, the adiabatic architecture features more transistors. We will show in this article how to make by combining approximation computation with adiabatic logic, energy-efficient, low-power, and small-area circuits are created (Figure 1). We'll explain how approximation circuits can fend off side-channel attacks like Differential Power Analysis when implemented using adiabatic logic (DPA).

As illustrated in this article, In order to estimate the total or carry output, the complete adder can use adiabatic logic on two rails this will make it easier to design energy utilized, less power consumption as well as enhance the secure designs with lower number of Tran's resistor. In this article, the TSAA and TCAA are two designs of approximation full adders that are discussed.

The Carryout is approximated by TSAA using the exact Sum, whereas the Sum is approximated by TCAA using the precise Carryout. Positive Feedback that is both secure and energy-effective utilized adiabatic logic is used to design the two approximation proposed adders. The adders design according to simulation data, a TSAA design In comparison to the previous system, EE-SPFAL saves money, has less inaccuracy, and occupies less space. TSAA based on EE-SPFAL is likewise shown to be more secure than TCAA which is also on the same basis of EE-SPFAL.

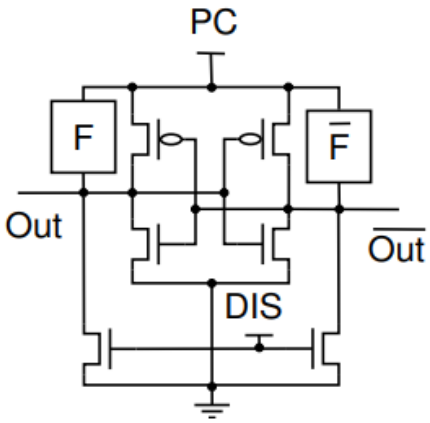


Fig2: EE-general SPFAL's schematic

With the rise of the Internet of Things, it is critical to Secure and energy efficient RFID and smart cards are examples of Internet-of-Things devices. The battery life improves as the security of these gadgets improves. Mobile gadgets that run on ultra-low power, battery life is a critical factor. Adiabatic logic is a new way for creating IoT devices that are both energy efficient and safe that does not sacrifice battery life. Adiabatic logic However, it has the disadvantage of being limited to a few MHz frequency range. Adiabatic logic, on the other hand, is a type of logic that is used to solve problems. Can be utilised to construct energy-efficient and safe low-frequency IoT devices like there are two sorts of smart cards: RFIDs and smart cards.

RFID tags, for example, use a 13.56 MHz frequency [5,] which is within the range of adiabatic logic's energy-efficient operation. Despite the fact despite the fact that adiabatic logic saves energy, Energy losses still exist (section II B). Quasi energy loss overcomes adiabatic power losses in limited

circuits [10]. EESPFAL, an energy-efficient and safe adiabatic logic that avoids non-adiabatic waste of energy, is the goal of this research. EE-SPFAL, a proposed adiabatic logic, can enhance RFID and swipe card security without simultaneously prolonging battery capacity.

When compared to earlier the quasi power dissipation of EE-SPFAL related logic circuits is much less, leading to higher total energy effectiveness of EE-SPFAL based circuits. Such circuit has been utilized to construct fundamental logic units such as buffers/inverters, AND/NAND, and XOR/XNOR gates, among others.

The proposed adiabatic logic family's security is ensured by a DPA attack on the S-box circuit, which was constructed using the EE-SPFAL gates. The secret of the DPA-resistant EE-SPFAL-based S-box circuit designs is revealed by a standard CMOS-based S-box circuit. When compared to SQAL and normal CMOS logic, SPICE simulations show that the EE-SPFAL-based S-box circuit saves up to 65 and 90 percent of energy at 12.5 MHz, respectively.

The energy dissipation of the EE-SPFAL based S-box circuit is compared to that of the SQAL based S-box circuit and the CMOS based S-box circuit to validate our results over a wide frequency range. We also constructed an Advanced Standard Encryption data channel of 8 bits, as mentioned in [6]. (AES) An on-the-fly key expansion mechanism is part of the architecture. We discovered that a single logic-based EE-SPFAL cycle can save you a significant amount of time. Processing may work with a variety of plain text inputs. The AES design uses the same amount of electricity all the time.

***Adiabatic logic:***

With the use of power clocks, adiabatic logic recycles the charge in the load capacitor. Charge recycling has helped to reduce the loss of dynamic switching energy caused by adiabatic logic. Figure 1 shows how load capacitors are charged and discharged adiabatically. In an adiabatic circuit, the energy wasted is computed as follows when a continuous current source provides the charge,

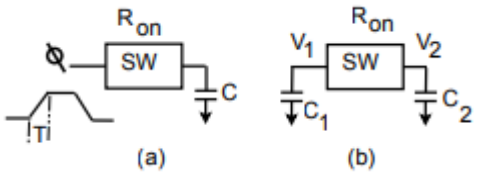


Figure-3: The model type of switch a) loss due to adiabatic cooling b) loss that is not adiabatic

$$E_{diss} = \frac{RC}{T} C V_{dd}^2$$

T represents the capacitor's charging and discharging period. The load capacitor is C, and Vdd is the full swing of the power clock. If T 2RC is used as a time constant, the adiabatic circuit consumes less energy than a standard CMOS circuit. Even though adiabatic circuits lessen they still suffer from various sorts of energy losses due to dynamic switching.

***In adiabatic logic, there are losses:***

In adiabatic circuits, there are two types of non-leakage energy losses: adiabatic and non-adiabatic.

1) Figure 1 illustrates the adiabatic loss. (a) To replicate adiabatic loss, a switch model was utilised. When the switch (SW) is turned on, it displays the adiabatic loss.

$$E_{adiabatic} = \frac{R_{on} C_L}{T} C V_{dd}^2$$

The switch's ON-resistance is Ron, and its transition time is T, and the load capacitance is CL. The adiabatic loss vanishes as the transition period (T) approaches infinity. In practise, it's impossible to get T is the amount of time it takes for something to undergo a change. As just a reason, adiabatic loss cannot be avoided.

2) Non-adiabatic loss: To demonstrate non-adiabatic loss, a switch model is employed shown in Figure 1(b). If there is a voltage differential between the two terminals when Non-adiabatic loss happens when the switch is turned on. It's a loss due to adiabatic cooling,

$$E_{non-adiabatic} = \frac{1}{2} \frac{C_1 C_2}{C_1 + C_2} (V_1 - V_2)^2$$

The supply just at two nodel junctions right even before device is switched on are V1 and V2, respectively, and the probable correlates are C1 and C2 of the pair of nodes linked to the switch, respectively. Quasi adiabatic degradation is much bigger than adiabatic loss in low-speed working circuits [10]. To avoid non-adiabatic loss, the transistor should not turn on when there is a potential difference between the drain and the source.

***Previous research has been done on DPA-resistant adiabatic logic:***

Only a few small reversible logic groups have ever been documented in the literature as being able to withstand the DPA attack: SAL, SyAL, and CSSAL [14] are all acronyms for the same thing. Among the DPA-resistant adiabatic logic families proposed in the literature, Secured Quasi-Adiabatic Logic is the most cost-effective in terms of power consumption and overhead. During the examination of the outputs, however, SQAL suffers from non-adiabatic energy loss.

***Energy Recovery Principle:***

In current CMOS technology, the power supply supplies CL, CLV 2 dd to charge a capacitance output node. A transistor channel route wastes the other half of the CLV 2 dd energy, while CL stores half of it. Energy recovery circuits, unlike typical CMOS circuits, use the adiabatic switching principle to gradually charge the capacitance and recycle there is a charge at the conclusion of each cycle.

***Side-Channel Attacks Using Power Analysis:***

By utilising data collected from cryptographic equipment, side-channel attacks can expose the secret key. Attacks on the side channel include attacks on power, timing, and electromagnetics, to name a few. The three attacks utilised in power analysis are SPA, DPA, and CPA. SPA: To determine the cryptographic approach a gadget employs, an attacker examines its power consumption. DPA: A side-channel attack that uses statistical analysis of the correlation between processed data and power traces to uncover the secret key of a cryptographic device. To discover the correct key, CPA as like as DPA it upgrades and calculates the statistical correlation coefficient between both the energy trace as well as readings of the key guess's intermediate result. In order to identify the hidden key, these attacks are supplemented using speculative power models.

## II. EARLIER WORK

In approximation edge computing, the use of adiabatic logic could assist reduce energy while also improving security against attacks from the side Two approximation adders based on adiabatic logic are presented as a case study to demonstrate the benefits of approximation computation in combination with adiabatic logic. To shrink the overall size and usage of energy, the dual-rail feature of adiabatic logic is utilised in the proposed approximation adders. In comparison to a CMOS-based AMA, TSAA and TCAA Use fewer transistors while using adiabatic logic. At some MHz operating frequency and 45 nm technology node, the adiabatic TSAA and TCAA showed significant power and energy savings over the conventional CMOS AMA. Both proposed architectures are also more resistant to DPA assaults, as demonstrated.

Adiabatic logic and approximation computation are two new techniques for creating low-power circuits. Accuracy is a trade-off in approximate computing to save space. It appears to be promising for IoT edge device error-tolerant programmes. Cyber security solutions, on the other hand, have not yet been adequately addressed [3, 4]. According to [3,] an approximation the adder's output and power consumption have a positive relationship that increases as the mistake rate increases. Non-approximation circuits, such as cryptography, run at lower frequencies and supply voltages than approximate circuits, making reverse engineering easier [4]. In order to attack the approximation

circuits, adversaries could employ techniques like as side-channel attack and reverse engineering.

The sum or carry output of a complete adder can be approximated using this article demonstrates dual-rail logic. This would enable us to create designs with lower number of transistors which are energy-efficient, low-power, and secure. TSAA and TCAA are two approximate full adder designs discussed in this article produce Output and Output, respectively. TSAA uses the precise Sum to approximate the Carryout, whereas TCAA uses the precise Carryout to approximate the Sum.

Positive Feedback that is both energy-efficient and secure the two approximation adders are implemented using adiabatic logic [7]. (EE-SPFAL). According to the simulation results, Compared to a TSAA based on EESPFAL, A TCAA developed on the basis of EE-SPFAL it reduces the expenditure, is more consistent, and is smaller. A TSAA based on EE-SPFAL, according to our findings is also more secure than a TCAA.

EE-SPFAL (Adiabatic Logic with Energy-Efficient Safe Positive Feedback) [7] [Adiabatic Logic with Energy-Efficient Safe Positive Feedback] [Energy-Efficient Safe Positive Feedback Adiabatic is a low-power, safe adiabatic logic family. EE-SPFAL uses a consistent amount of power and is resistant to DPA assaults. Figure 2 shows how Blocks F and $\bar{F}$ The EE-SPFAL architecture is used to create the results and the results a more thorough discussion of adiabatic logic can be found in a recent study [6]. The AAA comes in two flavours, both based on EE-SPFAL.

F and Fbar, respectively, create output and output (Fig. 2). As a result, the two recommended adders use complementary outputs to mimic to reduce overall size, power, and energy consumption, combine or carry-out outputs. As a consequence, two approximated adders were developed using equations 1 and 2: TCAA and TSAA are two different forms of approximation adders.

**F = Sum**

**Fbar = Sumbar = Cout --- (1)**

**F = Cout**

**Fbar = Coutbar= Sum --- (2)**

***Approximate True Sum Adder:***

Cout is known as Sumbar complement in the TSAA scheme, which is based on the EE-SPFAL. Using the dual-rail capability of adiabatic logic, Cout was created as a supplement to Sum (Equation 3). As a result, there is no longer a requirement Cout and Coutbar are calculated separately in a separate circuit.

**SumT SAA = A ⊕ B ⊕ C**

**Cout T SAA = SumTSAAbar ---------- (3)**

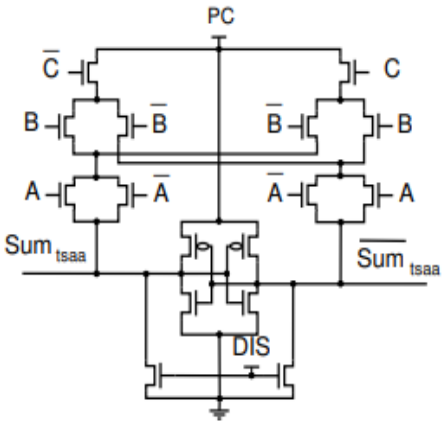


Fig 4: Proposed design of EE-SPFAL-based TSAA.

***True Carry Out Approximate Adder:***

The TCAA schematic is based on the EE-SPFAL standard, is shown in Figure 5. CoutTCAAbar is how SumTSAA is calculated in TCAA (Equation 4). As a result, a separate circuit for the Sum output is no longer needed.

**Cout TCAA = B.C + A.C + A.B**

**SumT CAA = CoutTCAAbar ----------(4)**

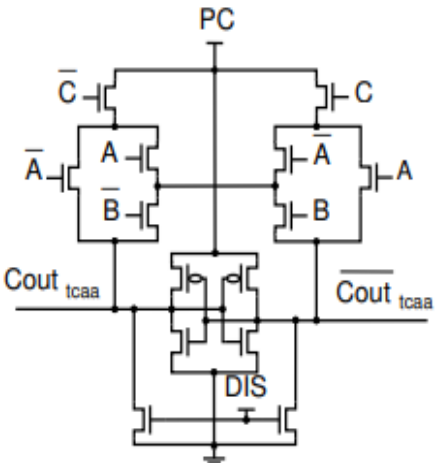

Fig 5: Proposed design of on TCAA based on EESPFAL

## III. PROPOSED WORK

By reusing the energy Adiabatic logic, which is stored in the load capacitor, allows for energy-efficient computing [6]. Families of adiabatic logic predominantly dual-rail in nature. As a result, in comparison to regular CMOS, the adiabatic architecture features more transistors. We will show in this article how to make by combining approximation computation with adiabatic logic, energy-efficient, low-power, and small-area circuits are created (Figure 1). We'll explain how approximation circuits can fend off side-channel attacks like Differential Power Analysis when implemented using adiabatic logic (DPA).

This article demonstrates how a complete adder can approximate employing for the sum or carry output, Arithmetic logic using two rails Creating energy-efficient, low-power, and secure circuits will be easier with fewer transistors. In this post, we'll look at two approximate full adder designs: the TCAA and TSAA are two different types of approximate adders.

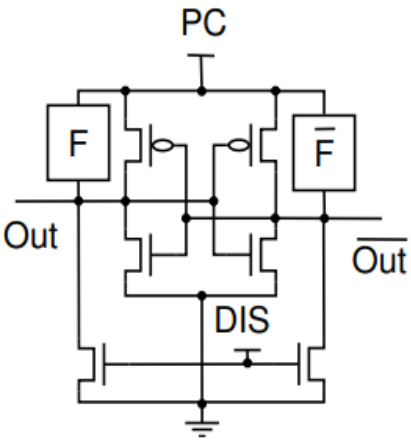


Fig 6: EE-SPFAL schematic in general

With the rise of the Internet of Things, it is critical to create secure and energy efficient IoT devices include RFID tags and smart cards. The battery life of these devices improves as the security of these devices improves. Mobile devices with ultralow power consumption, battery life is critical. Adiabatic circuitry is a new technology for making Iot technologies that are really power efficient as well as secured even while preserving battery performance. The frequency the adiabatic logic range is limited to a few MHz, which is a drawback. However, adiabatic logic can be utilised to design energy-efficient and secure low-frequency IoT devices such as RFIDs and smart cards.

RFID tags, for example, operate at 13.56 MHz [5,] which is within the range of adiabatic logic's energy-efficient operation. Despite the fact despite the fact that adiabatic logic saves energy, it still has loss of energy (section II B). In low-speed circuits [10], The energy loss caused by non-adiabatic processes is greater than the energy loss caused by adiabatic processes. The goal of this report is to build EESPFAL, an energy-efficient and safe adiabatic logic that can improve energy efficiency by eliminating non-adiabatic energy loss. EE-SPFAL is a proposed adiabatic logic that can improve RFID and smart card security while simultaneously improving battery life.

***True Sum Approximate Adder:***

Cout is the Sum complement in the TSAA scheme, which is based on the EE-SPFAL. Using the dual-rail capability of adiabatic logic, Cout was created as a supplement to Sum (Equation 3). As a result, calculating Cout and Coutbar no longer necessitates the use of a separate circuit.

$$\text{SumT SAA} = A \oplus B \oplus C$$

$$\text{Cout T SAA} = \text{SumTSAAbar} \quad \text{---------- (3)}$$

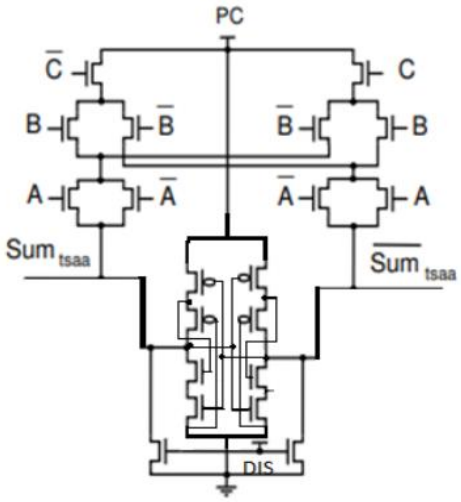


Fig 7: TSAA based on the EE-SPFAL.

***Approximate Adder True Carry Out (TCAA):***

The TCAA scheme based on EE-SPFAL is shown in Figure 4. SumTSAA is calculated in TCAA as CoutTCAAbar (Equation 4). As a result, the Sum output no longer requires a separate circuit.

**Cout TCAA = B.C + A.C + A.B**

**Sum TCAA = CoutTCAAbar ---------- (4)**

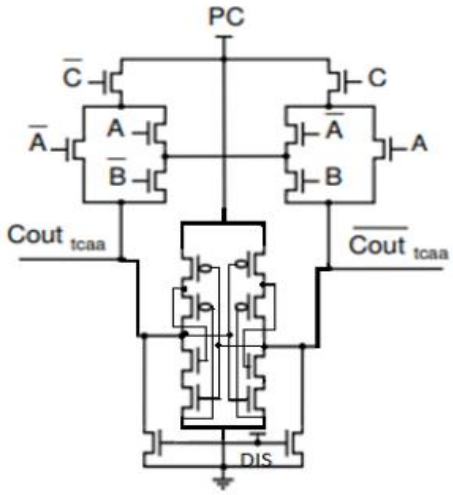


Fig 8: The EE-SPFAL is used to create a TCAA

## IV. EXPERIMENTAL RESULTS

The comparison of the proposed design is done for the design of TSAA and TCAA with newly proposed design of lector approach based TSAA & TCAA by using the EE-SPFAL.So this section uses EESPFAL used for the purposes of comparison, we employed TSAA and TCAA, CMOS-related AMA [8], and CMOS-used approximation mirror adders (AMA) [9]. The power, energy, area, and security from DPA hacks of these produced designs are all compared. The 45 nm approach was used to run the simulations. PMOS has a width of two times that of NMOS for CMOS simulation, whereas NMOS has a width of 250 nm. PMOS has a width of twice in nm in the EE-SPFAL simulation, but NMOS has a width of 180 nm.

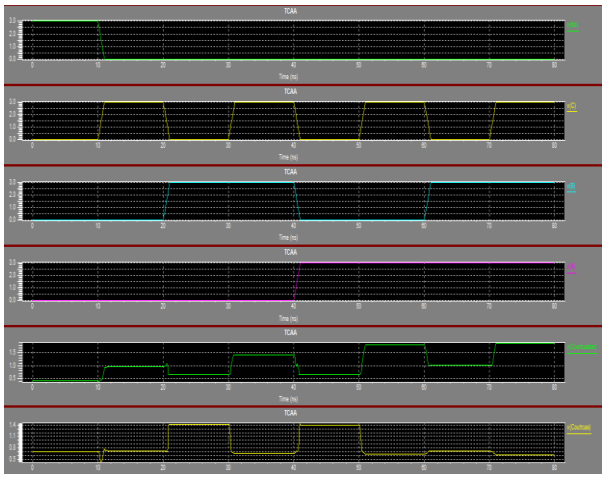

Fig 13: TCAA output waveforms using EE-SPFAL.

## V.CONCLUSION

We established the feasibility of low-power, secure edge computing devices by integrating approximation computing and adiabatic logic with the lector approach. Two novel adiabatic approximation adders are proposed in this study, both based on adiabatic logic with two rails when adiabatic logic-based approximation adders are compared to traditional CMOS architecture, the findings show significant power and energy savings. They are unaffected by the DPA. The adiabatic TCAA employs fewer transistors and consumes less energy than the conventional TCAA. The adiabatic True Sum Approximate Adder is less effective against DPA assaults.

## V. REFERENCES

[1]. P. Mohanty, According to IEEE Consumer Electronics Magazine, the internet of everything (ioe) age needs security and privacy by design.., vol. 9, no. 2, pp. 4–5, 2020.

[2]. Satyanarayanan, The emergence of edge computing, Computer, vol. 50, no. 1, pp. 30–39, 2017.
[3]. Yellu, N. Boskov, M. A. Kinsy, and Q. Yu, Security threats in approximate computing systems, in Proceedings of the 2019 on Great Lakes Symposium on VLSI, 2019, pp. 387–392.
[4]. Regazzoni, C. Alippi, and I. Polian, Security: the dark side of approximate computing? in 2018 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). IEEE, 2018, pp. 1–6.
[5]. Gao, Q. Wang, M. T. Arafin, Y. Lyu, and G. Qu, Approximate computing for low power and security in the internet of things, Computer, vol. 50, no. 6, pp. 27– 34, 2017.
[6]. Kahleifeh and H. Thapliyal, Adiabatic logic based energy-efficient security for smart consumer electronics,IEEE Consumer Electronics Magazine, pp. 1–1, 2020.
[7]. D. Kumar, H. Thapliyal, and A. Mohammad, EESPFAL: A Novel Energy-Efficient Secure Positive Feedback Adiabatic Logic for DPA Resistant RFID and Smart Card, IEEE Transactions on Emerging Topics in Computing, vol. 7, no. 2, pp. 281–293, 2019.
[8]. Weste and D. Harris, CMOS VLSI Design: A Circuits and Systems Perspective, 4th ed. USA: Addison-Wesley Publishing Company, 2010.

**Cite this article as :**

Vikram Dhoni, Vilaskumar Patil, Veeresh Kumasigi, "Implementation of High-Speed Approximate Adiabatic Logic Using Lector Approach for Security Enhancement", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 9 Issue 4, pp. 353-360, July-August 2022.
Journal URL : https://ijsrst.com/IJSRST229451