International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:2 Volume No.10 March - April – 2026
DOI:10.46647/ijetms.2026.v10i02.020 ISSN: 2581-4621

ATTACK RESISTANT CIRCUIT DESIGN FOR CRYPTOGRAPHY

Er. Nuli Namassivaya[1], Manas Viswanauth Prathi[2], Meghana Reddy Bessam[3], Sree Harshith Phani Madabushi[4]

[1]*Associate Professor & HOD, Electronics and Communication Engineering, MVSR Engineering College,* Hyderabad, India

[2,3,4]*Electronics and Communication Engineering, MVSR Engineering College,* Hyderabad, India

***Abstract*—**In the growing digital world network security takes highest priority.Cryptograhic data protection is equally needed from hardware and software attacks. This research presents Binary Decision Diagram (BDD)-based dual-rail logic circuit schemes designed to mitigate power analysis attacks (PAAs). The most important thing about our circuit schemes is that each circuit path has the same number of switchings. The transistors are connected in such a way that they can pull up and pull down outputs based on binary decisions made from the input variables.Cryptographic algorithms like the Advanced Encryption Standard (AES) have become widely used due to the growing need for secure data transmission in embedded systems. However, side-channel attacks, especially power analysis attacks, can affect AES hardware implementations. The design and implementation of an AES encryption system on FPGA with secure inter-board communication via the Serial Peripheral Interface (SPI) protocol are presented in this paper. The suggested system resists simple side-channel leakage and shows dependable data transfer between two FPGA boards without changing output logic. Verilog HDL is used to implement the design, and hardware testing and simulation are used to validate it. The system is appropriate for secure embedded applications since experimental results verify proper encryption functionality and successful data transfer across FPGA boards.

***Keywords*—** Advanced Encryption Security (AES), Binary Decision Diagram(BDD),Dual-rail logic ,FPGA, SPI Protocol, Side-Channel Attacks, Verilog HDL, Cryptographic Hardware

INTRODUCTION

The difference in power dissipation is a major factor in whether a power analysis attack works or not. Dynamic power, which is a big part of total power consumption, depends on how much the transistors switch, which in turn depends on the input combinations that are sent to the transistors. The current goes from the voltage source to the ground through capacitors in transistor networks, but not directly. This depends on how often the transistors switch [1]. Charging or discharging the output capacitors makes outputs. Current dual-rail complementary circuit implementations of logic functions engineered for power attack resilience exhibit asymmetry in the critical paths between charge flow points. In this study, our goal is to find circuit structures that are resistant to power attacks, timing attacks, and early propagation effects so that we can get good attack resistance with the same critical path lengths for all possible switching paths. This property may confer immunity to timing attacks, provided that the execution of the underlying algorithm is not data-dependent, thereby precluding the initiation of timing attacks. The Boolean function of the input variables is used to build the pull-up and pull-down circuits that are needed. So, BDD-based logic synthesis can be used to make these pull-up and pull-down networks of transistors.

This project uses Binary Decision Diagram (BDD) logic on an FPGA platform to create a secure hardware version of an AES S-Box [1]. The design's main goal is to make it less likely that side-channel attacks will work by using a structured decision-tree approach instead of traditional lookup tables. To process the chosen input bits and create the right substitution value, a simplified BDD structure is used [1]. To make things safer, a dual-rail encoding method is used, which gives both true and complementary outputs. A pre-charge mechanism is added to set outputs to a fixed state before each evaluation cycle, which keeps switching activity balanced.The design is written in Verilog and put together so that it can be used on an FPGA board. A testbench is used to do

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:2 Volume No.10 March - April – 2026
DOI:10.46647/ijetms.2026.v10i02.020 ISSN: 2581-4621

functional verification by checking that the system works correctly with different combinations of inputs. The output behavior shows that the dual-rail logic keeps the integrity of the complementary signals. The method shows how hardware-level design methods can stop information from leaking through power lines. In general, the project shows a safe and effective way to use cryptographic primitives in systems based on FPGAs.

Serial Peripheral Interface (SPI) protocol to send messages between two FPGA boards. SPI is a synchronous serial communication protocol that lets a master and a slave device send data back and forth at high speeds. One FPGA is set up as the SPI master and the other as the SPI slave in this design. The master starts the conversation and controls the clock signal, while the slave responds to the data that was sent.Data is transmitted serially using the MOSI line, synchronized with the clock signal generated by the master. A chip select signal is used to enable communication with the slave device. The SPI master converts parallel data into a serial stream, while the SPI slave reconstructs it back into parallel form. The design ensures reliable communication through proper timing and synchronization. The system is implemented using Verilog and deployed on FPGA boards using PMOD interface pins. Simulation and hardware testing confirm correct data transmission between the two boards. The received data is displayed on LEDs, validating the communication process.

RELATED WORK

In recent times, the focus in the design and implementation of secure cryptographic hardware has moved away from traditional post-silicon mitigation techniques and towards the development of novel pre-silicon design and synthesis techniques that inherently prevent side-channel leakage. For instance, traditional logic styles like dual rail with pre-charge (DRP), which inherently try to keep the power consumption constant, have been coupled with modern automated synthesis techniques like PoSyn [2]. The latter technique optimizes the bipartite mapping between RTL components and standard cells to minimize mutual information leakage. In addition to these synthesis approaches, powerful statistical distinguishers like Mutual Information Analysis (MIA) have emerged as powerful tools for identifying various types of dependencies, including non-linear ones, in the device's side-channel information [3]. These tools are more robust than the commonly used Pearson correlation method, especially in situations where the model of the device's leakage is not very accurate. Further, specific circuit designs based on Balanced Binary Decision Diagrams (BDD) have also been developed to equalize the length of paths in the transistors as well as the outputs, effectively countering power analysis as well as EPE attacks [4] .These integrated approaches demonstrate that the integration of secure synthesis, invariant logic styles, and information-theoretic analysis can effectively limit the success rates of Differential Power Analysis (DPA) and Correlation Power Analysis (CPA) without compromising efficiency in terms of area and performance.

methodology

Leakage Assessment of Cryptographic Operations

An initial evaluation of side-channel vulnerabilities was carried out through the use of MATLAB. At this stage, Correlation Power Analysis was employed to assess the extent to which power consumption can reveal secret information through the process of encryption. Simulated power analysis was conducted through the use of intermediate values from the encryption process, with a focus on S-box calculations. Statistical correlation was then employed to assess the correlation between the power consumption and the possible keys, demonstrating the process through which secret keys can be revealed.

For the analysis of the simulated power traces obtained during the cryptographic processes, the Difference of Means (DoM) method was utilized. The power traces were divided into two cohorts depending on the predicted value of the intermediate bit (such as the output of the S-Box). The average power consumption was then calculated for each cohort. Finally, the difference between the two averages was computed to obtain the leakage patterns.By observing the peaks of the difference of means plot, the locations of the maximum information leakage can be determined. This shows

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:2 Volume No.10 March - April – 2026
DOI:10.46647/ijetms.2026.v10i02.020 ISSN: 2581-4621

how the attacker can potentially obtain the secret key information using the power consumption variation

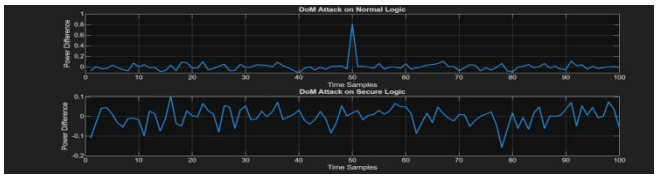

Fig 1 .Difference of Mean(DOM) of basic AES s-box and BDD based AES s-box

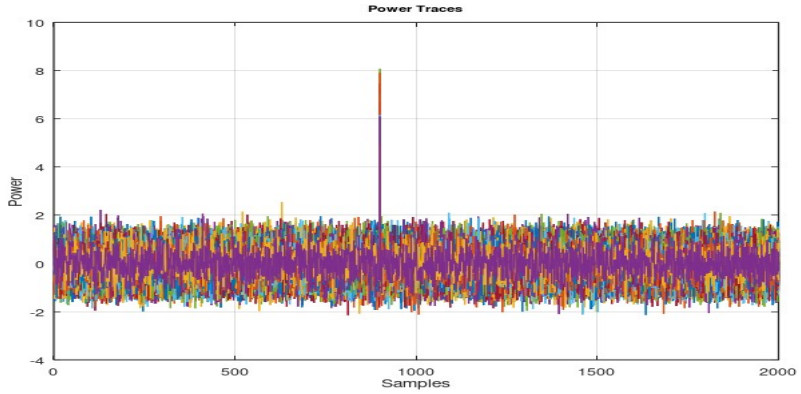

Fig 2 .Correlation Power Analysis(CPA) for basic AES s-box

B BDD-Based Secure AES S-Box Design

The entire design is specified using the Verilog HDL and is subjected to synthesis using FPGA design tools. Functional verification is also performed using a testbench that stimulates the design with different combinations of inputs and checks the accuracy of the outputs [4]. Once the verification is complete, the design is implemented on the FPGA device, and the output signals are monitored using LEDs. The correctness of the dual rail logic is confirmed by checking whether the XOR of out_t and out_f is always a bit pattern of ones.

To improve the level of security, dual rail logic is incorporated into the design. For a given output, both the true value, represented by "out_t," and the false value, represented by "out_f," are obtained. The power dissipation is thus uniform, irrespective of the values being processed [5]. A precharge operation is carried out before the evaluation process. The actual operation is carried out during the evaluation process, which ensures uniform switching activity between the cycles.

The design is coded using the Verilog HDL. The design is then synthesized using FPGA design tools. Functional verification is done by developing a testbench, which includes a wide range of input values. The design is then implemented on an FPGA, and the output values are observed through LEDs. The dual rail logic is verified by checking whether the XOR operation between "out_t" and "out_f" results in all ones.

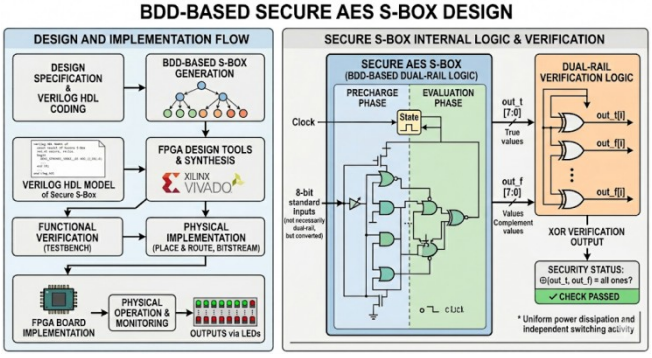

Fig 3 .Block diagram for BDD secure AES s-box

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:2 Volume No.10 March - April – 2026
DOI:10.46647/ijetms.2026.v10i02.020 ISSN: 2581-4621

C. SPI-Based Inter-FPGA Communication

The second phase of the project focuses on the establishment of communication between two FPGA boards by the Serial Peripheral Interface (SPI) protocol. The system is divided into two modules: the master module and the slave module. The master FPGA sends the data, generates the clock, and initiates the communication, and the slave FPGA receives the data and converts it to parallel form.For the purpose of ensuring proper communication, proper timing control and division of the clock are used to ensure the data transfer rate is compatible with the FPGA boards. The design is implemented using the Verilog language and simulated using testbenches to ensure proper data transfer between the master and slave blocks.

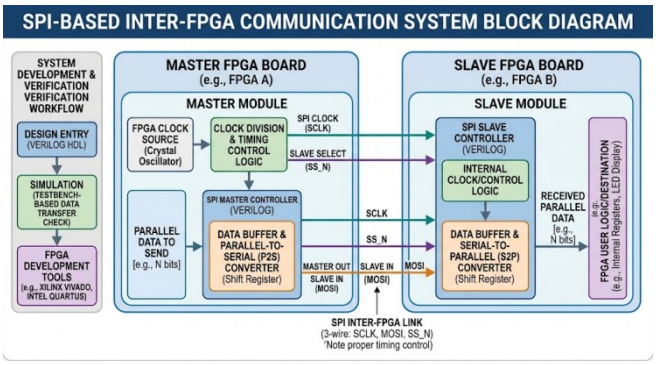

Fig 4 .SPI-based communication between two FPGA boards

D.Equations

Shannon's Expansion Equation

, Each node of our BDD logic works on this equation which lead us to the out_f and out_t values.

$F = x \cdot F_x + x' \square F_x$

F is any Boolean function

x is a Boolean variable

x′ is the complement (NOT) of x

F_x is the positive cofactor of F with respect to x, obtained by setting x = 1.

F_x' is the negative cofactor of F with respect to x, obtained by setting x = 0.

analysis

Simulation analysis of BDD bases AES s-box

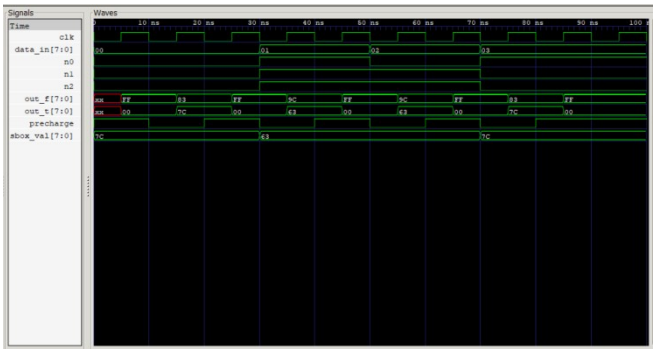

Fig 5 .BDD version simulation

The waveform illustrates the behavior of the dual rail outputs, namely out_t and out_f, along with the precharge signal. In every clock cycle, the outputs display a similar behavior, and the relationship between the outputs is always complementary. In particular, for every change in the data_in signal, the corresponding outputs are produced so that the XOR between out_t and out_f results in all ones. This property is important for reducing the impact of Correlation Power Analysis (CPA) because CPA relies on the varying power consumption caused by the data-dependent switching activity. In the proposed implementation, the invariant number of transitions is maintained irrespective of the data, which eliminates the correlation between the data and the power

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:2 Volume No.10 March - April – 2026
DOI:10.46647/ijetms.2026.v10i02.020 ISSN: 2581-4621

consumption. Therefore, the peaks in the correlation obtained from several power traces used for extracting the keys are significantly reduced.

In addition to mitigating CPA, the above waveform also demonstrates the effectiveness of the precharge mechanism in mitigating side-channel attacks. Before the actual evaluation phase of each computation cycle, the precharge signal initializes both the out_t and out_f lines to a known state, usually zero or a balanced state. This guarantees that every computation cycle begins from the same electrical state, thereby avoiding any data dependence on previous operations. When the evaluation phase begins, both lines switch simultaneously, thereby making all bits switch at the same time. This balances the switching activity of all bits, making it difficult for attackers who try to perform Difference of Means (DoM) or Domain-Oriented Masking (DOM) attacks based on the differences in average power consumption between different data classes. As all bits switch at the same time, the difference in the average power consumed by different data classes is minimized.

Furthermore, the structured design through the BDD approach greatly improves the overall security of the design. Unlike the usual S-box design that relies on a look-up table, the BDD approach ensures a more deterministic signal transition, thus reducing the effects of data-dependent changes in logical activity. The waveform clearly indicates that signal transition is under control and is consistent for all possible input combinations, which is a desirable trait for side-channel analysis. The use of dual rail and pre-charge logic ensures a design that limits temporal and spatial variations in signal transitions. As a result, both CPA and DOM attacks become useless, as the distinguishing characteristics necessary for analysis are absent. The approach clearly demonstrates the importance of meticulous design in hardware development, which can significantly improve side-channel resistance without compromising functionality.

Implementation of BDD based AES s-box on FPGA

The design of a dual-rail circuit allows for an equal number of transitions on the two outputs of each rail, which creates an even distribution of switching activity [4]. By maintaining an even distribution of switching on both rails, the Hamming weight of the total output will not change(out_t $\oplus$ out_f consistently results in all ones)and will therefore not vary based on the value of the input data. It is important to keep an even distribution between the two rails because doing so will reduce any potential exploitation of leakage caused by power consumption being dependent on how much power is consumed by a transitioned state. When all outputs produce an equivalent number of transitions each cycle, there are no preferential data patterns that create an inherent bias towards one data pattern over another. Thus, the use of statistical methods to analyze differences in power consumption due to correlated data patterns (e.g., Correlation Power Analysis (CPA)) will no longer be effective. This demonstrates the ability to reduce the potential for side-channel attacks by using dual-rail designs in hardware production[6].

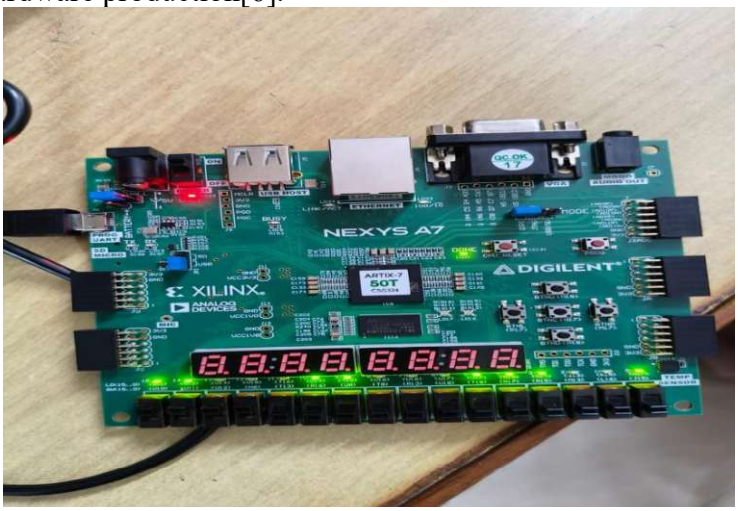

Fig 6 .Hardware implementation of BDD on FPGA

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:2 Volume No.10 March - April – 2026
DOI:10.46647/ijetms.2026.v10i02.020 ISSN: 2581-4621

The figure above has
Input -8'b 10000001
Out_t - 8'b 11000110
Out_f - 8'b 00111001
XORing the values out_t and out_f we get a constant hamming weight, representing the security of the data in transmission

SPI Communication between two FPGA boards

This design employs a master/slave (SPI - Serial Peripheral Interface) arrangement for communication between both FPGA boards (a master controlling all data transmission). The SPI master FPGA will provide both the serial clock (SCLK) and generate all the time-based signals associated with transmitting data on the master-out/slave-in (MOSI) line. The onboard clock of the FPGA (approximately 100 MHz) is divided down using a clock divider to generate a more stable/slower SPI clock. An SPI clock will be located between several hundred kilohertz and several megahertz so that both boards can communicate reliably without having their communication disrupted due to timing violations.

Data is transmitted in a serial shift register format using a 16 bit packet being sent one bit at a time per clock cycle. The bit rate for the system is equal to the SPI clock frequency, which means if the SPI clock is set to 1MHz, the system's bit rate will be 1 Mbps. Therefore, the SPI link's bandwidth (maximum transfer rate) will be approximately equal to the bit rate for example if the SPI Link clock were to be 1 MHz, then the bandwidth would be about 1 Mbps.

This bandwidth identifies how rapidly data packets can be sent between two FPGA boards. Sampled at the edge of the clock, the slave will sample incoming data allowing proper synchronization and correct recreation of the data stream being transmitted.

From a system perspective, the Synchronous Peripheral Interface (SPI) communication method provides a good balance between performance and simplicity. In SPI communications, the effective bandwidth of the SPI communication system is directly related to the clock frequency of operation and the size of the packet being transmitted. For example, as the size of the packet increases, the number of clock cycles required to transmit the packet also increases. Although the effective bandwidth increases with increased SPI clock frequency, there are also physical limits to the ability to maintain reliable communication at high frequencies due to constraints such as signal integrity, noise and wire latency. The SPI frequency used in this implementation has been optimized for reliable data transfer and not for maximum throughput. Timing violations and resulting data corruption are prevented by ensuring the specified amounts of setup and hold time are met. Overall, SPI communications provide a stable bandwidth that is appropriate for transferring data between FPGAs while providing the required synchronization and reliable signal integrity.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:2 Volume No.10 March - April – 2026
DOI:10.46647/ijetms.2026.v10i02.020 ISSN: 2581-4621

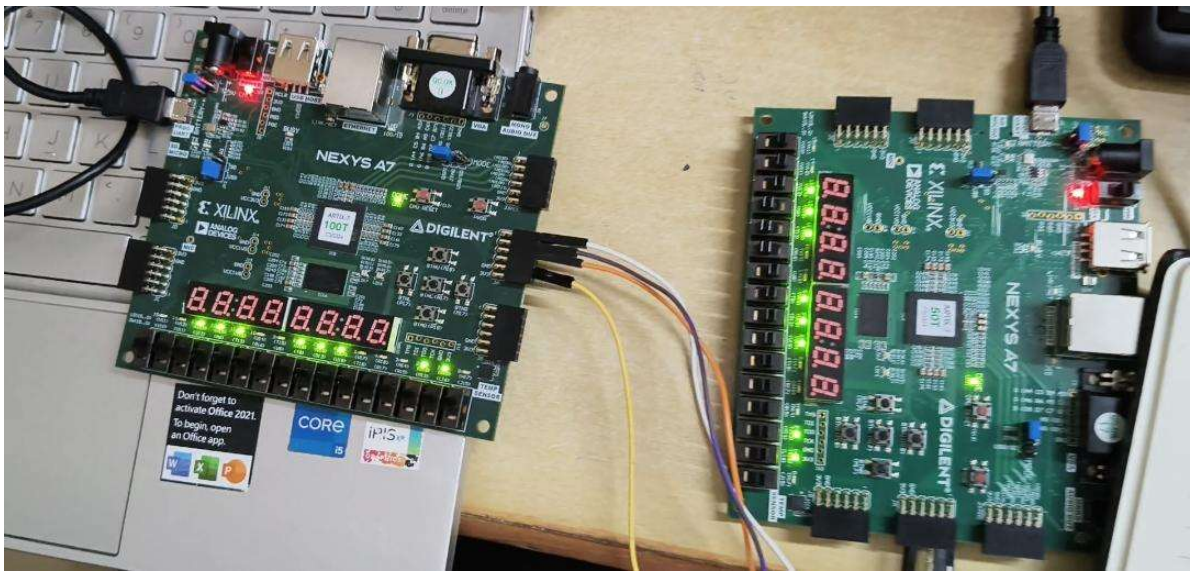

Fig 7 .SPI protocol between FPGA boards

CONCLUSION

Synthesis results of a BDD-based AES S-Box implementation have shown that the design has an effective balance between security and hardware resource utilization. The Binary Decision Diagram approach uses a decision tree structure for computations and thus reduces redundant logic operations, which ultimately optimizes the use of LUTs and logic elements on FPGAs [1]. The dual-rail implementation guarantees balanced switching activity of both true and complement outputs, which helps maintain constant Hamming weight, greatly reducing data-dependent power variations and therefore improving resistance to side-channel attacks. The pre-charge mechanism also contributes to achieving a uniform initialization before each evaluation cycle and reduces leakage[4]. The synthesis report exhibits stable timing performance with no observable critical violations and substantiates reliable operation at the targeted clock frequency. In summary, the BDD-based design is a secure and efficient solution for providing hardware implementations of cryptographic applications that require protection against power analysis attacks.

The communication method used by the two FPGA boards through this SPI interface is both reliable and effective for transmitting secure information. The method provides reliable transfer of information between the two boards at a controlled bit rate where the high frequency system clock is divided to yield a stable SPI clock frequency, maintaining synchronized data transferred across the interface. The SPI clock frequency sets the total communication bandwidth (bytes transferred per second), providing an optimum tradeoff between the speed of communication and the integrity of the transmitted signal. Data is transferred at a moderate bit rate rather than at the maximum feasible rate; therefore, less abrupt switching activity occurs, and reduced high frequency noise is generated, thus minimizing the risk of exploitation via power-based side channel attacks. In addition, because of the assignment of uniform and clock driven data, the timing of each signal transition during the data transfer is predictable and consistent, which reduces the amount of variation in the data's power usage that may depend on the content of the data. As a result, it will be significantly more difficult for an attacker to obtain useful information from either board by using techniques such as Correlation Power Analysis or Difference of Means. In addition, the use of structured packet sized transfers with logical timing boundaries enforced by the chip select signal across the interface also provide additional stability to the communication between the two boards. Ultimately, by choosing a bit rate and bandwidth that provides reliable communication between the

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:2 Volume No.10 March - April – 2026
DOI:10.46647/ijetms.2026.v10i02.020 ISSN: 2581-4621

two FPGAs, it also helps to minimize the potential for side channel leakage and thereby achieves the overall security objectives of the system.

Feature	**Basic AES S-Box**	**Balanced Dual-Rail S-Box**	**BDD-Based Secure S-Box**
Logic style	Single-ended	Dual-rail dynamic	Balanced BDD dynamic
Precharge–Evaluate	No	Yes	Yes
Complementary outputs	No	Yes	Yes
Switching activity	Data-dependent	Constant magnitude	Constant & uniform
Evaluation path	Input-dependent	Partially uniform	Fully uniform
Timing uniformity	No	Partial	Yes
Glitch/early propagation	Present	Reduced	Eliminated
Power leakage	High	Medium	Low
EM leakage	High	Medium	Low
Resistance to SCA	Weak	Moderate	Strong
Area& complexity	Low	Medium	High
Overall security	Poor	Moderate	High

Table 1 :Comparison of types of AES s-box

References

[1] Parth De, "DESIGN OF POWER ATTACK RESISTANT CIRCUITS FOR CRYPTOGRAPHY", Thesis(M.S),Dept.of Computer science Engineering , IIT Kharagpur, August 2014.
[2] Amisha Srivastava,Samit S. Miftah, " PoSyn: Secure Power Side-Channel Aware Synthesi, arXiv:2506.08252v1, June 2025
[3] Nicolas Veyrat-Charvillon, Fran¸cois-Xavier Standaert "Mutual Information Analysis: How, When and Why?", UCL Crypto Group,Universit´e catholique de Louvain, B-1348 Louvain-la-Neuve.
[4] F.Standaert ct al.,"UnifiedFrameworkfor the Analysis of Side-ChannclKcy Recovcry Attacks. Annual International Conference on the Theory and Applicalions of Cryptographic1echmigue (EUROCRYP1),2009
[5] D.Oswald and C.Paar. Side Channel Analysis Channel Analysis:Attacks and Counter measurcs in Introduction to Cryptography, Sprnger,2011.
[6]N.A.Said,S.A.Hussien,andM.T.Sultan,"Hardware Implementation of AES with Power Side Channel Attack Rcsistance."/IEEEAccess,vol.9,pp.12345-12360,2021