ISSN: 2278-4632
Vol-11 Issue-02 2021

IMPLEMENTATION OF AES ENCRYPTION IP

Dr.Mohini Prasad Mishra[1], Dr. Prakash Pathak[2]
[1](Department of CSE,Gandhi Engineering College, Bhubaneswar)
[2](Department of CSE,Gandhi Engineering College, Bhubaneswar)

ABSTRACT

Security plays a vital role in Digital Circuits and Applications. The Integration of Crypto processors with the hardware is inevitable and must. Crypto processors are used in military application, ATM, smart cards, SIM cards, automobiles and so on. In this project We Implemented AES ENCRYPTOR IP, Intellectual property (IP) is a reusable logic unit or layout design that is normally developed with the idea of licensing to multiple vendors for using as building blocks in different chip designs. The IP developed in the project performs 128-bit AES encryption and the technology involved is Synopsys's SAED 32nm static CMOS technology operating at nominal voltage of .95 V, temperature of-40° C and process of .99 which is a global slow corner and the design is finely tuned on Power, Performance, AREA (PPA) parameter. The target frequency for this AES Encryption IP is 0.714 GHz. Since the project deals with the nano transistors, the CAD tools are used for In-House deigning, Synopsys VCS and Icarus Verilog is used to simulate SOFT IP, Synopsys DC compiler is used to synthesis the FIRM IP and to Implement the final HARD IP Synopsys ICC compiler is used. Verilog Hardware descriptive language (HDL) is used to code the SOFT IP

Key words: ASIC, AES Encryption, Soft IP, Firm IP, Hard IP,
Verilog, Topographical mode, Physical design, Saed32 Technology

1. INTRODUCTION

Information Security has undergone major changes in the past and present times. Due to the advancement of the technology the whole world depends on computer, the data is stored in the computer, cloud, memory card, Hard disk drive and so on. There is a great threat to the data so, security is must for every individual and organization. Cryptography is a method to protect the data or information through codes or algorithms. The data is encrypted through cryptography algorithms and the key. The encrypted data can be decrypted through the suitable cryptography algorithm and the key. We can classify encryption algorithms mainly into two types based on the key that is private key and public key. Private key algorithm is also called as symmetric key algorithm having a single key for encryption and decryption whereas public key algorithm has separate key for encryption and decryption. In comparison with Asymmetric Key algorithms, the Symmetric key algorithms are most efficient and fast to the large amount of data. AES Algorithm is one of the popular Symmetric key algorithm and secure algorithm adopted by US National institute of Standard and Technology (NIST) in 2001.

In this paper the AES Encryption algorithm is implemented using SAED 32nm static CMOS technology as a reusable Intellectual property (IP) by VLSI and ASIC methods. The designed AES Encryption IP is finely tuned on Power, Performance and Area parameter. Any designer can reuse my AES 128-bit encryption Soft IP to integrate with new security algorithm or application and also the designer can target my soft IP to FPGAS or extend to Application Specific Integrated Chips (ASIC's) with different technology. Not only SOFT IP if any developer working with SAED32 technology with suitable library can reuse my FIRM and HARD IP, the FIRM IP provides the designer a gate level netlist with logical information like power consumption, area of the cells, performance and other physical correlation

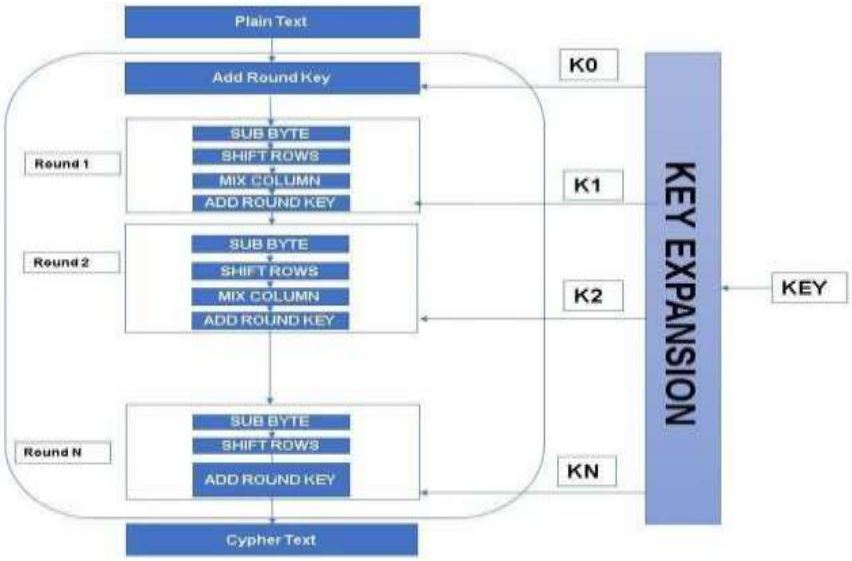
ISSN: 2278-4632
Vol-11 Issue-02 2021

information, whereas the final Hard IP give the final layout and designer can reuse it directly in his top-level security processor or crypto processor.

2. LITERATURE SURVEY

Advance Encryption Standard (AES) is a symmetric Key Algorithm. It is a block cipher which has a fixed plaintext of 128 bits and key size of either 128, 192, or 256 bits. It has 10, 12 or 14 rounds depending on the key length. The encryption process starts with the XOR operation between plain text and original key then the result will undergo 10, 12, 14 rounds to get cypher text. The architecture of each round consists of 4 sub blocks namely SubBytes, Shift Rows, Mix Columns, and AddRoundKey. AES processes data in byte sized chunks represented as a 4x4 matrix and the complete set of those data bytes are called the state. SubBytes is the process for replacing the byte by using the substitution boxes. Shift Rows shifts each row of the state matrix by a particular offset based on the row. In Mix Columns, the four bytes of each column is combined with an invertible linear transformation. Lastly, AddRoundKey XORs the current state with the Round Key. In the final round, there is no Mix Columns sub block [1]. The Figure 1 describes the architecture of AES Encryption Architecture. According to the architecture the Encryption block takes Plaintext and set of keys to get cypher text. If we are designing N round AES encryption Architecture then N round Keys are needed as an input. In this paper the AES IP has 10 rounds so it takes 10 round keys and plain text.

These Intellectual properties (IP) are reusable logic unit or layout design that is normally developed with the idea of licensing to multiple vendors for using as building blocks in different chip designs. There are three ways in which we can classify the IP and they are SOFT IP, FIRM IP, HARD IP. Soft IP cores are delivered as RTL VHDL/Verilog code to provide functional descriptions of IP's and provides maximum flexibility and re-configurability. But disadvantage is they must be synthesized, optimized before integration [2,3,4]. FIRM IP balances the high performance and optimization properties of the hard IPs with the flexibility of soft IP's. These cores are delivered in the form of targeted netlist for the specific physical libraries after performing synthesis without performing the physical layout. The designers can optimize cores for their specific design needs as the Firm IP blocks are have parameterized circuit descriptions. As the parameters are flexible, it allows the designers to make the performance more predictable [2,3,4]. Hard IP consists of hard layouts using particular design libraries and is delivered in masked-level designed blocks.



ISSN: 2278-4632
Vol-11 Issue-02 2021

Figure 1 AES Encryption Architecture

These cores give optimized design and the highest performance for the particular physical library. The main disadvantage of hard cores is they are technology dependent and also, they provide minimum flexibility and portability [2,3,4]. To tune the design and to get the great correlation for final layout the two pass ASIC Synthesis can be used which can be achieved by running the synthesis in Topographical mode. Once we design and verify the Verilog soft IP designer can Synthesize the netlist, the normal synthesis of the netlist involves translation of Verilog code into Boolean Logic, optimizing up the Boolean logic and matching the optimized Boolean logic with the technology library. In addition to the netlist and library the timing constraints need to be provided for normal synthesis and CAD Tool SYNOPSYS DC will calculates the delay based on cell delay and net delay, whereas in two pass synthesis Mode the Topographical Mode, the physical constraints like chip utilization ratio and aspect ratio should be provided so that the CAD Tool SYNOPSYS DC synthesize the netlist, then virtually place the cells , estimate the congestion and with the help of TLU and congestion data it will again Re-synthesize the highly correlated netlist with respect to Physical layout.

Implementing the final Physical Layout is done using physical design methods which involve Floor Plan, Power Plan, Placement of standard Cells, Clock Tree Synthesis (CTS), Routing.

3. PROPSED METHODOLGY

The design Approach can be done in three stages, first developing the Soft Ip, then Firm IP and then Hard IP. Following are the methods to Implement those three stages,

3.1. Soft IP Implementation Methodology

SOFT IP Implementation is done by developing Hardware descriptive Code for AES Encryption Architecture. In this project Verilog Hardware descriptive language is used. Mainly there are several rounds in AES Encryption Architecture and each round consist of four Sub blocks except the last round having only three Sub blocks. The sub blocks of Rounds are ADD ROUND KEY, MIX COLUMN, SHIFT ROWS and SUB BYTE. Based on its Architecture all of the SUB blocks should be coded in Verilog. The top-level block AES Encryption has 128 bits plain text, 10 round keys having 128 bits size and the clock as input and 128 bits cypher text as an output. The Figure 2 describes the top-level block diagram of AES Encryption

Figure 2 Top Level Block of AES Encryption IP

The Sub Byte block replaces the Bytes using its Substitution S- box tables and this can be implemented Using Case Construct in Verilog, Figure 3 is the picture of substitution table

ISSN: 2278-4632
Vol-11 Issue-02 2021

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8

Figure 3*:* Substitution transformation table

In the Mix columns, the four bytes of each column is combined with an invertible linear transformation to do so it is multiplied with constant matrix, the below Figure 4 is the picture of constant matrix and since the hexadecimal involved are 01, 02, 03 we can code multiplication logic exclusively for those three hexadecimals. The logics are mentioned below.

```
8'h01: outp = inp;
8'h02: outp = {inp[6:0],1'b0}^(8'h1b & {8{inp[7]}})
8'h03: outp = {inp[6:0],1'b0}^(8'h1b & {8{inp[7]}})^inp
```

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

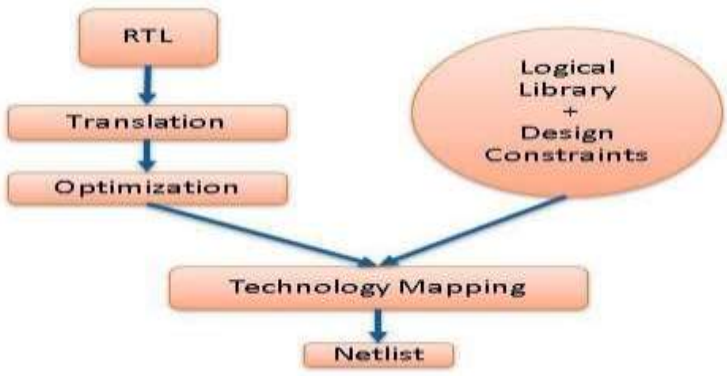
C

Figure 4: Constant Matrix used in Mix Columns

Coming to the ADD ROUND KEY It involves XOR operations so we can directly use XOR construct in the Verilog. Shift rows block can be implemented by wire assignment constructs.

3.2. Firm IP Implementation Methodology

The Objective of Firm IP is to get gate level netlist, the input required to generate netlist are Verilog, Logical Library, Timing constraints. If the implementation performed in Topographical mode, then along with the above inputs Milkyway references which contains physical data and TLU files are required to get RC net delay.



ISSN: 2278-4632
Vol-11 Issue-02 2021

Figure 5 General Netlist generation Flow

The general flows translate RTL to Boolean, then optimize the Boolean and then it will do technology mapping with the logical library based on Design constraints (timing constraints) to get netlist. In this project two pass synthesis methods are implemented using Synopsys DC Topographical mode. So, we need to provide milkyway references, TLU files and physical constraints like utilization and aspect ratio along with the above inputs, then DC synthesizes the netlist, does the virtual placement since, we provided physical library It can Place the physical cells and estimate the Congestion, then calculates accurate net delay with the help of TLU files and again it re-synthesizes the netlist with the accurate net delay. Figure 6 describes the Flow for DC Topographical mode and Figure 7 is the snapshot of Congestion of virtual placement of AES Encryption IP.

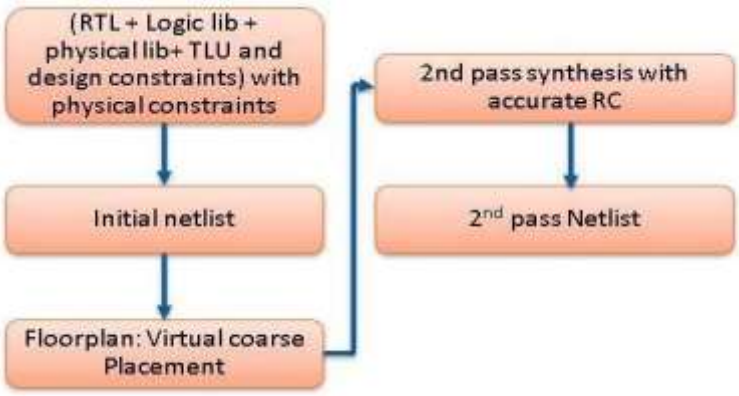
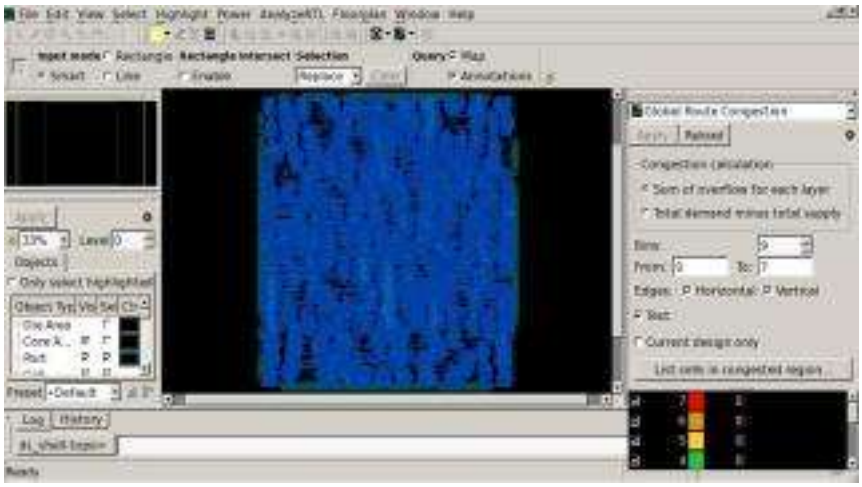


Figure 6: DC TOPOGRAPHICAL Flow



ISSN: 2278-4632
Vol-11 Issue-02 2021

Figure 7: Congestion Map of Virtual Placement

3.3. Hard IP Implementation Methodology

Implementation of a Hard Ip can be classified into following stages, Floorplan, Power-Plan, Placement, Clock Tree Synthesis and Routing. The Tool used in implementing Hard Ip is Synopsys ICC. The input required for implementation are netlist, design constraints (SDC), Logical library, Physical library, Technology file and TLU files.

Floorplan: In the floorplan stage size and shape of the Chip are estimated and apart from that we need to place the I/O pins and fix them, in order to estimate that we need to give aspect ratio and utilization ratio, here aspect ratio value is 1 which gives square shape and utilization ratio target is 80 %. The below Figure 8 is a snapshot of Floorplan of AES Encryption

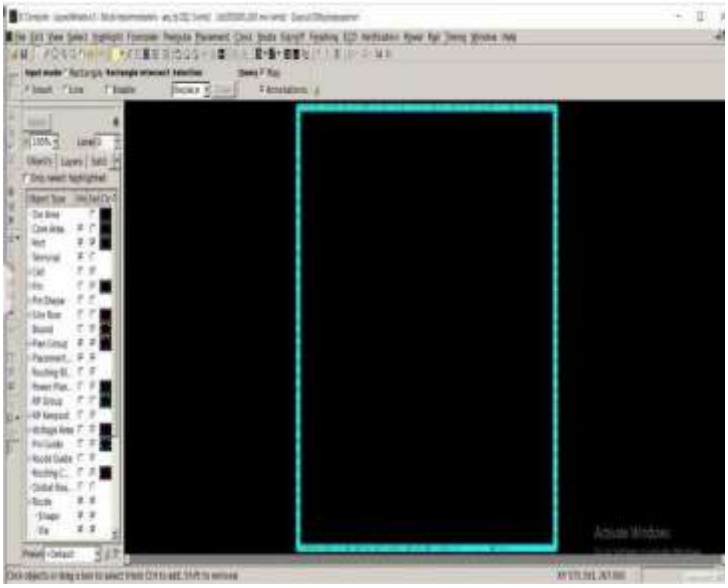


Figure 8: Floorplan of AES Encryption

Power Plan: In this stage we ensure power to the standard cells, this can be achieved by using mesh architecture. The mesh Architecture has VDD and VVS ring at the top level which brings powers from power pads and rings will supply to Power Straps and these power straps supply to standard cell rails. By this way standard cell sitting in the rail will get the power, since we are doing block level Implementation, we will be designing only straps and enabling the standard cell rail. The figure 9 describes straps and the standard cells rails are enabled but we need to zoom the design to see standard cell rails.

ISSN: 2278-4632
Vol-11 Issue-02 2021

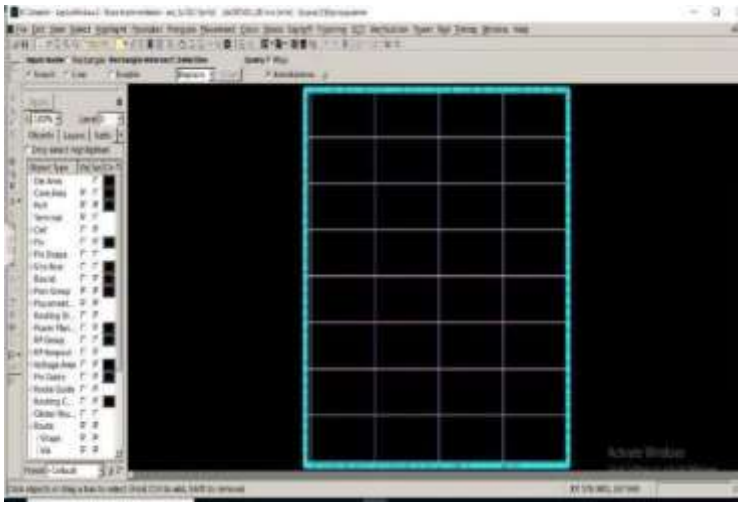


Figure 9: Power Straps of AES ENCRYPTION IP

Placement: It can be done in two steps first by coarse placing based on the option like timing, Congestion, power where cells can be overlapped and in the last step, tool does the legalized placement where cells are not overlapped and optimized based on option, in this project the placement is timing driven but it also tries to reduce the congestion to some extent. To design these straps M8 and M9 metals are used and it reduces IR and avoids EM, since those are higher metals and have more thickness than other metals. The Figure 10 describes the placement stage.

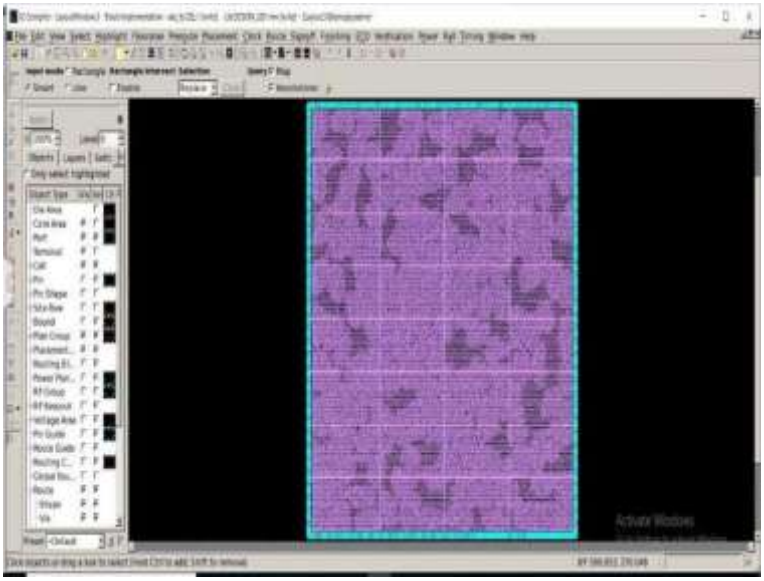


Figure 10: Placement stage of AES ENCRYPTION IP

Clock Tree Synthesis: In this stage all the flip flops are clocked by building the clock tree with help of Buffers and Inverters. For this stage we can mention the target skew, latency, metals for routing and other clock constraints like specific clock buffers, DRV and so on. If nothing mentioned tool takes default options during clock tree synthesis. The Figure 11 describes the Clock Tree of AES Encryption IP.

ISSN: 2278-4632
Vol-11 Issue-02 2021

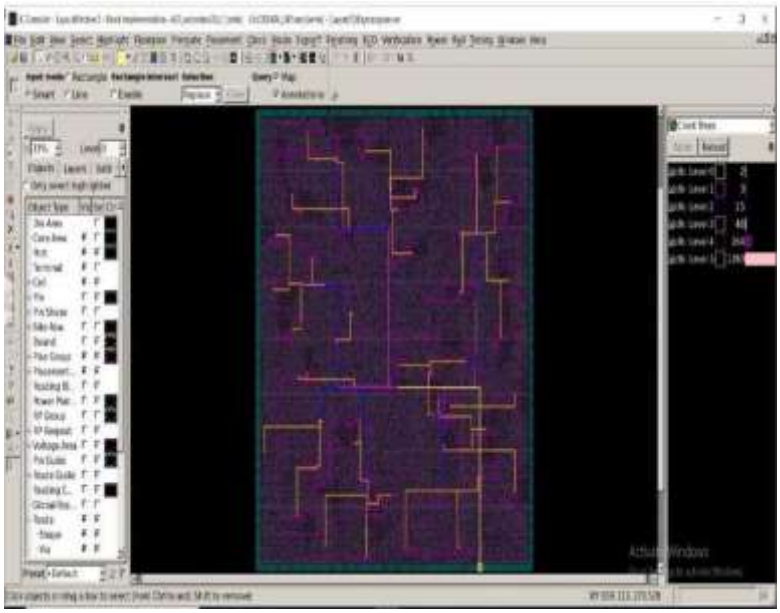


Figure 11: Clock Tree of AES ENCRYPTION IP

Routing: In this stage routing of nets takes place and it is done in three stage and they are global routing, track assignment and Detailed routing/search and repair. In global routing the nets are loosely assigned and based on congestion the nets are assigned whereas, in track assignment vertical and horizontal tracks are assigned and at the Detailed routing/search and repair the nets are routed and DRC are removed. To optimize the Quality of Results (QOR) of the design we can go incremental routing optimization. The Figure 12 describes the final Routed Layout of AES Encryption IP.

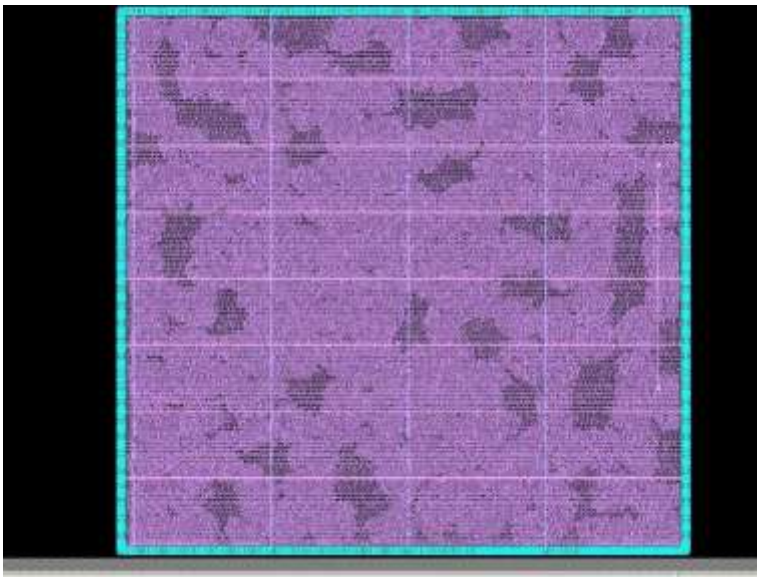


Figure 12: Final Routed Layout of AES ENCRYPTION IP

4. RESULTS AND DISCUSSION

The Soft IP, FIRM IP and HARD IP are synthesized using Static CMOS SAED 32 Technology. Design is finely tuned on Performance, Power and Area parameter. The SOFT IP are simulated against the Testbench and verified. The Figure 13 is the simulated results of the SOFT IP and the design is simulated using Icarus Verilog simulator

ISSN: 2278-4632
Vol-11 Issue-02 2021

ISSN: 2278-4632
Vol-11 Issue-02 2021

Figure 15: SOFT IP Simulation Results 1

The Slack of the Gate Level netlist (FIRM IP) is positive and it is listed in the table 1. Slack is the difference between actual time and the required time for a timing path.

Table 1 Timing report

Timing path Groups	Register to Register	Register to Output	Input to Register	Input to output
slack	0 ns	0.27 ns	0 ns	0.47 ns

The power and area of the netlist is are listed below in the Table 2. As we see the netlist consumes power of 21.78 mw and area of 169190.27 ^{2} .

Table 2 Power and Area report of the netlist

Power and Area report of the netlist	
Total Power	21.78 mW
Dynamic Power	15.4 mW
Leakage Power	6.3 mW
Cell Area	169190.27^2
Combinational Cells Area	160275.66^2
Non-Combinational Cells Area	8914.60^2
Buffer/ Inverter Cell Area	12393.84^2

The final technical reports of Hard IP are listed below in the Table 3,4,5 and 6, they are categorized into General, Timing, Area and Power specification. As we see the netlist and the final routed Chip have a great Correlation and it is due to Topographical synthesis.

Table 3: General Report of AES Encryption IP

General Reports	
Functionality	Performs 128- bit AES Encryption
Technology	28nm Static CMOS SAED32
Library type	Current Composite Source (CCS)
Operating Voltage	0.95 V
Operating Temperature	-40.0 C
Process	0.99

ISSN: 2278-4632
Vol-11 Issue-02 2021

ISSN: 2278-4632
Vol-11 Issue-02 2021

Table 4: Timing Report of AES Encryption IP

Timing Reports	
Clock Frequency	0.714 GHz
Worst Negative Slack	0 ns
Total Negative Slack	0 ns
Number of Violating End points	0
Skew	0.023 ns
Longest Path Delay	0.284 ns
Shortest Path Delay	0.260 ns

Table 5: Area Report of AES Encryption IP

Area Reports	
Chip Area	832975 um^2
Standard CELL Area	694052 um^2
Utilization Ratio	83.32%

Table 6: Power Report of AES Encryption IP

Power Reports	
Total power	27.07 mW
Dynamic Power	20.70 mW
Leakage Power	6.372 mW

5. SCOPE FOR THE IMPROVEMENT

Since this paper deals only with the design part, there are lot of things can be done like performing Verification, Linting, Validation, Adding the DFT logics, parasitic extraction and timing signoff, we also can perform Fill insertion, DFM MAS checks, DFM Pattern optimization. In the design methodology we can go for Multi-Mode and Multi corners also where multiple of operating conditions, constraints are taken together. The Digital IC Implementation is a vast topic and this paper concentrates only on design aspects.

6. CONCLUSION

A High performance AESENCRYPTION IP is Implemented and it performs 128 -bit AES encryption and the Chip has better Performance, Power, Area and the netlist and final chip has great correlation. Since it works around 0.714 GHz it Qualifies to integrate with Consumer grade chip or High- Performance Chip. The following IP has Very good Quality of Results with zero timing violations, better Utilization of 83.32% and power of 27.07mW. Anyone can reuse my Soft IP and those who working on SAED 32 technology can reuse my FIRM and HARD IP. As mentioned before the Chip operates at 0.95V voltage, -40C temperature and at slow process of 0.99.

REFERENCES

[1] Y. Chou and S. L. Lu, "A High Performance, Low Energy, Compact Masked 128-Bit AES in 22nm CMOS Technology," 2019 International Symposium on VLSI Design, Automation and Test (VLSI- DAT), 2019, pp. 1-4, doi: 10.1109/VLSI- DAT.2019.8741835.

[2] S, Sindhu & A M, Vijaya Prakash A M & K V, Ankit. (2015). ASIC Implementation of I2C Master Bus Controller Firm IP Core. International Journal of VLSI Design & Communication Systems. 6. 51- 63. 10.5121/vlsic.2015.6405.

ISSN: 2278-4632
Vol-11 Issue-02 2021

[3] Marcello Dalpasso, Alessandro Bogliolo, and Luca Benini,(2000) “Hardware/Software IP protection.” In Proceedings of the 37th Design Automation Conference, pp.593-596, June.

[4] Mandeep Singh, Balwinder Singh, (2012) “Microcontroller Based Testing of Digital IP- Core” International Journal of VLSI design & Communication Systems (VLSICS) Vol.3, No.2.