CHAPTER 5

PROPOSED AES ARCHITECTURES FOR HIGH EFFICIENCY

High speed architectures are the current research interest in cryptographic algorithms, but the limitations imposed by the hardware makes it essential to design an optimized architecture. Although many implementations of AES algorithm are relatively efficient when implemented in software, there is always a need for cryptographic processor, which has high throughput and low area and power (Shylashree 2012). Different applications need different Speed/Area Trade off, hence this research work discusses possible implementations of AES which improves its performance characteristics.

From the analysis made in chapter 3 and 4, it is found that the Folded Parallel SubPipelined architecture gave high throughput and Mux based SBox and MixColumn had low area.

Part of the work reported in this chapter has been submitted for Review as under:

Under Review

Communicated
Optimized architectures can be obtained by combining the high throughput architecture (Folded PSP) and low area techniques (Mux Based SBox and MixColumn) proposed and implemented in the previous chapters. These proposed optimized structures include

- **Integrated Folded PSP**
  
  This architecture is the integration of area optimized SBox and MixColumn with Folded Parallel Subpipelining architecture.

- **Compact AES Architecture**
  
  Compact architecture uses looping technique to design an optimized architecture.

The following sections present the design and an implementation technique of the above proposed research works.

### 5.1 PROPOSED INTEGRATED FOLDED PSP ARCHITECTURE

With the rapid growth in the field of wireless communication standards, the need for integration of high speed and small core encryption is gaining importance. An AES architecture, implementation which satisfies both the goals, ie., small area consumption and high throughput conditions is proposed in this research work. As already discussed in previous chapters, Folded Parallel Sub Pipelined architecture had highest throughput of 69.9 Gbps and Internal transformations like SBox and MixColumn when modified using Multiplexer gave the minimum number of slices.

Implementing these structures on FPGA is expected to provide higher flexibility for limited resource systems like mobile phones. An optimized AES architecture is designed by integrating the Folded PSP architecture with the structurally modified SBox and MixColumn and is presented in Fig 5.1. In this
architecture, the input 128 bit plain text is divided into 4 words of 32 bits each P1, P2, P3, P4. As in Fig 5.1, the primary inputs (Plain Text P1, P2, P3, P4) are XORed with the Round Key values (K1, K2, K3, K4) in the precomputation round.

Fig 5.1 Integrated Folded PSP Architecture

The output of precomputation round is arranged in the state array and is processed in bytes. Each round, in this case 10 rounds, follows the same set of
transformations like SubByte, ShiftRows, MixColumn and AddRoundKey. In the proposed architecture inclusion of the folded structure eliminates the need for a ShiftRow operation (in all the rounds) and the input bytes should be selected such that the functionality does not change. The order of input values chosen are \{A, F, K, P\}, \{E, J, O, D\}, \{I, N, C, H\} and \{M, B, G, L\}.

The SubByte operation uses the proposed Mux Based SBox instead of the normal LUT / CFA based Sbox. This reduces the area and delay involved in locating the value to be substituted. Similarly, the normal xtime based MixColumn is replaced with the proposed Mux Based MixColumn to reduce the area. AddRoundKey operation involves XOR operation with the round keys generated by the key generation unit. The key generation technique can be either on the fly or can use stored values. In this research work, round keys are generated earlier and stored in a register to reduce the time required for generating key at each round (Frank Vater 2007).

Thus the proposed Integrated Folded PSP (InFo PSP) occupies less area and has better processing rate, which increases the overall efficiency of the architecture. The proposed InFo PSP architecture was designed and implemented in Virtex 6 XC6VLX75T device. This program was simulated using ModelSim 6.5 and synthesized in Xilinx 13.1.

The simulation waveform of the proposed Integrated Folded PSP architecture is shown in Fig 5.2. The encryption block is simulated with an input data and key length of 128 bits. The input data are entered as 4 input blocks each with 32 bits. The four input blocks are \{00112233\}, \{44556677\}, \{8899AABB\}, \{CCDDEEFF\} and the input key is \{000102030405060708090A0B0C0D0E0F\}. There will be 10 rounds for AES-128. The output of the tenth round is the cipher text.
Fig 5.2 Simulation Waveform of Integrated Folded Parallel SubPipelined Encryption

The encrypted cipher output is taken as encrypt1, encrypt2, encrypt3, encrypt4. The four encrypted output blocks are \{69C4E0D8\}, \{6A7B0430\}, \{D8CDB780\}, \{70B4C55A\}. This cipher is given as the input for the decryption. The simulated waveform of AES decryption is shown in Fig 5.3.

The decryption block is also simulated with an input data and key length of 128 bits. The input data are entered as 4 blocks which was the output of encryption. The Key Expansion is the same for encryption and decryption process. The output of the tenth round of decryption will be plain text. The decrypted output is \{00112233\}, \{44556677\}, \{8899AABB\}, \{CCDDEEFF\} which is same as that
of the input data. The input values given are based on FIPS’197 (NIST 2001) and the output values are verified.

![Simulation Waveform of Integrated Folded Parallel Subpipelined Decryption]

Performance parameters are computed based on the synthesis report generated from the simulated code. Throughput analysis of this proposed architecture is performed based on the timing summary which gives the maximum frequency. Area in terms of slices occupied is noted from design summary. The total slices occupied out of the available slices are also displayed in design summary. The performance parameters thus found is compared with the existing techniques and is shown in Fig 5.4.
Device utilization summary: **INTEGRATED FOLDED PSP**

---------------------------

Device utilization summary:

---------------------------

Selected Device: 6vlx75tff484-2

Slice Logic Utilization:

Number of Slice Registers: 5248 out of 93120  5%

---------------------------

Timing Summary:

----------

Speed Grade: -2

Minimum period: 1.580ns (Maximum Frequency: 632.811MHz)

Yi Wang (2013) in their work implemented Masked AES architecture, which had a throughput of 40.9 Gbps. The proposed InFo PSP had a throughput of **80.9 Gbps, which is almost double the highest throughput**. The number of Slices occupied by Yi Wang is 9071 with 400 BRAMs. As discussed earlier, the number of slices occupied by each BRAM is 128 and hence the total area occupied by the design of Yi Wang is 60271 Slices. **The proposed InFo PSP occupies only 5248 slices** which is comparatively low.

Another work by Zhang (2010) had a throughput of 34.7 Gbps, which is low compared to the throughput of proposed InFo PSP architecture (80.9 Gbps). The total number of slices occupied by the architecture proposed by Zhang is 27989 including the BRAM used. Hence the proposed Integrated Folded PSP architecture has high throughput and low area when implemented on Virtex 6 Device.
The proposed InFo PSP architecture has better efficiency (Throughput / Slice) 14.9 Mbps when implemented on Virtex 6 Device. Efficiency can be improved further if the area is reduced. For this a compact AES architecture is designed and discussed in the next section.

5.2 PROPOSED COMPACT AES ARCHITECTURE

Looped or the iterative architecture uses the concept of feedback in which the architecture reuses the available hardware for ‘n’ number of times. In this work, AES uses 128 bit key, hence the same hardware can be used for 10 rounds. But this architecture is considered slow since output is obtained after 10 rounds. In this proposed work, looping concept is extended to obtain low area high throughput AES structure. This becomes possible by using Folded Parallel Subpipelined architecture in the loop, with the modified Sbox and MixColumn, integrated with it. The structure of the proposed architecture is presented in Fig 5.5.
A compact AES structure which was proposed by Chodowiec (2003) is reused in this proposed architecture. The difficulty in implementing a pipelined structure in looped network is that, pipelining uses registers to store data and reuse in the next stage, but a looped structure uses the concept of feedback. However, VHDL provides the option of clearly selecting the required bits of data to be processed after satisfying the required conditions. The logic structure used to perform this operation is a multiplexer. This proposed Compact AES architecture also includes replacing the Substitution Box with the proposed Mux based SBox and MixColumn with Proposed Mux based MixColumn. This further reduced the number of slices occupied.

![Fig.5.5 Compact AES Architecture](image-url)
The working of the proposed architecture is described based on two steps.

- **Key scheduling**
  The pre-computed Round Keys are generated by the Key Generation Module and stored in register which can be used for AddRoundKey operation. In this architecture, the round keys of 128 bits are divided into four 32 bits and are XORed with Plain Text inputs during the AddRoundKey transformation.

- **AES Encryption**
  As described in the Folded PSP architecture, the input 128 bits are divided into four 32 bit inputs. These bits are arranged such that the ShiftRow transformation is eliminated.

**Working:**

- Read the input in A, execute SubBytes operation using the proposed Mux Based SBox, and write the result to the corresponding register in MixColumn. MixColumn is replaced with the proposed Mux Based MixColumn. Perform AddRoundKey operation on this output with the Roundkey generated by the key generation module.

- Repeat for F, K, P input register, execute SubBytes, and then MixColumn for the result, perform AddRoundKey operation, and write the 4-byte result to the output memory, addressed in 0, 1, 2, and 3, (A, E, I, M) respectively.

- Repeat the above operations for input registers E, J, O and D in the same way. Write the result to the output registers addressed in 4, 5, 6, and 7, (B, F, J, N) respectively.

- Next, repeat for input registers I, N, C and H in the same way, and write the result to the output registers, addressed in 8, 9, A, and B (C, G, K, O), respectively.

- Finally, for input registers M, B, G and L the same process is repeated and the results are stored in registers, addressed in C, D, E, and F (D, H, L, P), respectively.
This set of four 32 bits forms the resultant cipher text after 10 rounds of operation else, the values of output register are given as input for the next round of operations.

Thus the low area implementation techniques of Mux Bases SBox and Mux Based MixColumn are integrated into the Folded Parallel Subpipelined architecture and this structure is rolled to get a compact structure. This architecture is coded using VHDL and implemented on Virtex 6 FPGA. ModelSim is used for Simulation and Xilinx is used for Synthesis. Based on the synthesis report, the performance parameters are computed and compared with the existing works. The simulation waveform of the proposed Compact AES encryption is shown in Fig 5.6.
The design summary of the Compact AES Architecture is given below:

Device utilization summary: **COMPACT AES ARCHITECTURE**

Device utilization summary:

Selected Device: 6vcx75tff484-2
Slice Logic Utilization:
Number of Slice Registers: 1888 out of 93120 2%

Timing Summary:

Speed Grade: -2
Minimum period: 2.402ns (Maximum Frequency: 416.308MHz)

The performance comparison chart of Compact AES Architecture is shown in Fig 5.7. A detailed study has been done on the existing architectures and the best of the available values are compared with the proposed techniques.

![Performance Comparison Chart for Compact AES Architecture](image_url)

**Fig 5.7** Performance Comparison Chart for Compact AES Architecture.
Yi Wang (2013) in their work obtained throughput of 40.9 Gbps by implementing Masked AES using different levels of pipelining. The proposed Compact AES Architecture achieved a throughput of 53.2 Gbps with a frequency of 416.3 MHz. The number of Slices occupied by Yi Wang is 9071 with 400 BRAMs. The proposed Compact AES occupies only 1888 slices which is the lowest value. This architecture has better efficiency (Throughput / Slice) 28.1Mbps when implemented on Virtex 6 Device.

➢ Comparison of Proposed Architectures

This research work has proposed architectures to increase the throughput through architectural modifications and decrease area through structural modification techniques. To design an optimized architecture with better efficiency, two integrated structures were proposed. All the proposed architectures were simulated and synthesized to calculate the performance characteristics. Performance Characteristics include Throughput, Area and Efficiency. A comparison chart for the characteristics of the proposed architectures is presented in Fig 5.8.

Of the architecturally modified techniques, folded parallel architecture has the minimum area in terms of slices. PSP architecture had a maximum area, however the folded PSP architecture had higher throughput with comparatively less area. All the architecturally modified proposed architectures were implemented using LUT based SBox and Xtime based MixColumn. The structurally modified Mux based SBox and Mux based MixColumn were integrated in the folded PSP architecture to implement InFo PSP which had the highest throughput of 80.9 Gbps. The same architecture was looped to create the Compact AES architecture which had a minimum area of 1888 slices. The integrated structures had a better efficiency compared to other proposed architectures.
Advanced Encryption Standard is the widely used symmetric key cryptographic algorithm for which different architectures were implemented to increase its performance. There are various hardware implementation techniques to increase the throughput and reduce the area. The proposed Folded Parallel, PSP, Folded Parallel SubPipelined architecture, Integrated Folded Subpipelined Architecture and the Compact AES architecture are compared for the parameters like area, frequency, throughput and efficiency and presented in Table 5.1.

Zhang et al (2010) had implemented AES architecture by pipelining concept. The area (in Slices) is recorded as 2389 which is lower than the proposed architectures. But the work of Zhang included 200 BRAMs in their design, which makes the total number of slices as 27989. The highest number of slices of all the proposed techniques is 7514, occupied by the PSP architecture. The lowest area occupied of all the proposed structures is by the Compact AES architecture (1888 Slices).
Table 5.1 Parametric Comparison of Proposed Techniques with Existing Architectures

<table>
<thead>
<tr>
<th>Author</th>
<th>Architecture Used</th>
<th>Area (Slices)</th>
<th>Frequency (MHz)</th>
<th>Throughput (Gbps)</th>
<th>Efficiency (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yoo et al (2005)</td>
<td>Parallel Pipeline</td>
<td>6541</td>
<td>222.187</td>
<td>28.44</td>
<td>4.34</td>
</tr>
<tr>
<td>Zhang et al (2010)</td>
<td>Pipeline</td>
<td>2389</td>
<td>271.15</td>
<td>34.7</td>
<td>14.5</td>
</tr>
<tr>
<td></td>
<td>Sub-pipeline</td>
<td>8896</td>
<td>202.265</td>
<td>25.89</td>
<td>2.91</td>
</tr>
<tr>
<td>Yi Wang et al (2013)</td>
<td>Pipeline</td>
<td>9071</td>
<td>319.9</td>
<td>40.9</td>
<td>4.51</td>
</tr>
<tr>
<td><strong>PROPOSED TECHNIQUES</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Folded Parallel</td>
<td>2688</td>
<td>368.6</td>
<td>37.1</td>
<td>17.5</td>
<td></td>
</tr>
<tr>
<td>PSP</td>
<td>7514</td>
<td>450.05</td>
<td>59.5</td>
<td>7.9</td>
<td></td>
</tr>
<tr>
<td>Folded PSP</td>
<td>6656</td>
<td>546.16</td>
<td>69.9</td>
<td>10.5</td>
<td></td>
</tr>
<tr>
<td>Integrated</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Folded PSP</td>
<td>5428</td>
<td>632.8</td>
<td>80.9</td>
<td>14.9</td>
<td></td>
</tr>
<tr>
<td>Compact AES</td>
<td>1888</td>
<td>412.8</td>
<td>53.2</td>
<td>28.1</td>
<td></td>
</tr>
</tbody>
</table>

Yi Wang (2013) in their work obtained a throughput of 40.9 Gbps by masking the pipelined AES architecture. This throughput value is slightly higher than the proposed folded parallel architecture, but the area occupied by the design of Yi Wang is 9071 which is much higher than 2688 slices occupied by Folded parallel structure. The highest throughput achieved is by the proposed Integrated Folded PSP (80.9 Gbps).
The efficiency of all the proposed architectures is computed and they are found to be better than that of the existing works. **Compact AES architecture has the highest efficiency of 28.1 Mbps.**

### 5.3 SUMMARY

 Efficient implementation of AES algorithm is well suited for applications which require flexible hardware implementation. Two architectures were designed and implemented to provide better efficiency. Based on the synthesized results, the following conclusions are made.

- Proposed Integrated Folded PSP architecture has the highest throughput (80.9 Gbps).
- Proposed Compact AES architecture has the lowest area in terms of slices (1888 Slices).
- Both the proposed architectures have better efficiency (**InFo PSP: 14.9Mbps, Compact AES: 28.1Mbps**)  

Design, development and implementation of high throughput and low area architectures were presented. The choice of these architectures is left to the consumer based on the requirement and the applications. The next chapter presents the overall contribution and the conclusion of this research work.