CHAPTER 6

CONCLUSION AND FUTURE SCOPE

6.1 SUMMARY

The first chapter of the thesis highlights the need and types of cryptographic systems in network security. Selection of performance parameters for a cryptographic algorithm such as Speed, Resources, Cost and Security aspects were discussed. The challenges faced during the design process such as, decreasing the critical path, maintaining the functionality when implemented in hardware/software were highlighted. A detailed review of the existing architectural and structural modification techniques applied to AES algorithm was presented in the second chapter. Detailed description of the existing techniques like Pipelining, SubPipelining, Parallel Processing, Folding and Iteration were presented.

Based on the challenges faced by the existing techniques, new architectures with better performance characteristics are designed and implemented in this research work. All the proposed works, namely Design of High Throughput Architecture, Design of Low Area Transformations and Design of Optimized AES Architectures, were verified and validated based on the data available in the NIST-FIPS 197 (NIST 2001). The proposed AES architectures were coded using VHDL and implemented on Virtex 6 FPGA.
Design of High Throughput Architectures

The first objective of this research work is to design and develop high throughput architectures for AES algorithm using Architectural modifications. The techniques involved in design and implementation were discussed in Chapter 3. Three AES architectures were developed to increase the throughput through architectural modifications.

Folded Parallel Architecture

In Folded Parallel architecture, processing rate was improved by performing computation in parallel, which also led to increase in size of the core. Hence parallel processing was combined with folding technique to reduce the area. This architecture was implemented in Virtex XC2VP70 and the throughput of the proposed architecture is **32.34 Gbps** while the throughput of the design by S.M. Yoo (2005) is **29.77 Gbps**. The throughput obtained by this architecture increased to **37.1 Gbps** when implemented in Virtex 6 device while the area occupied is **2688 Slices**. Folded parallel architecture design was also implemented in various available FPGAs and the throughput, thus obtained was compared with the highest values in literature. The proposed architecture obtained better throughput when compared to the existing techniques in all the devices as processing 32 bit data in four different blocks increased the encryption rate. Further increase in throughput is possible if the critical path can be reduced.

Parallel SubPipelined Architecture

In the proposed PSP architecture, a combination of fine grain pipelining with parallel processing is used to further increase the throughput. Subpipelining reduces the critical path by inserting buffers in the round
transformations, while parallel processing technique processes multiple data at the same time. The throughput of the proposed architecture, when implemented using Virtex XC2VP70 FPGA was **36.38 Gbps** by the design by Zhang (2010) while the highest throughput obtained by the existing techniques using the same device is **34.7 Gbps**. The throughput obtained is still higher when implemented in Virtex 6 device (**Throughput: 59.5 Gbps, Area: 7514 Slices**). This proposed architecture was also implemented in other FPGAs and the throughput, thus obtained is compared with that of the existing techniques and is found to be higher. To decrease the area occupied, folding technique can be used as in Proposed Folded PSP.

- **Folded Parallel SubPipeline Architecture**

  Folded PSP architecture is designed to further increase the throughput with lesser area. This architecture uses folding structure in PSP to reduce the complications involved in routing and this structure eliminated the need for ShiftRow operation. Thus the total number of slices reduces and also the delay. When implemented in XC2VP70 device, the highest throughput in the literature is **34.7 Gbps** obtained by the design of Zhang (2010) while the proposed Folded PSP attained a throughput of **38.86 Gbps** in the same device. The throughput obtained after implementing this architecture in Virtex 6 is **69.9 Gbps** while the area occupied is **6656 Slices** which is lesser than the PSP architecture. Folded PSP Architecture had the highest throughput among these proposed techniques as none of the internal components remain idle in this architecture.

  All the above mentioned architectures were coded in VHDL and implemented on Virtex 6 FPGA. Comparison of these architectures was done with the existing techniques and it was found that the throughput of the proposed techniques were higher. Among the proposed architectures based on architectural modifications, **Folded PSP** architecture has the highest throughput with optimum
area. This architecture can be used for high speed applications and can be further modified to get better efficiency through Structural Modifications.

✓ **Design of Low Area Transformations**

The second objective of this research work is to reduce the area through structural modifications applied to the internal transformations of the AES algorithm. The transformations chosen are the SubByte and MixColumn based on the complexity involved in implementing these transformations. The proposed techniques and the results obtained were demonstrated in Chapter 4. Structural modification techniques are applied to SBox and MixColumn transformations to reduce the area through resource sharing techniques.

➢ **Mux Based SBox**

In the proposed Mux Based SBox, Multiplexers were used to select the predefined SBox values. In this technique, 16x16 SBox is divided into four 8x8 LUTs containing the 256 values. Each of these LUTs is selected by using the select bits in the position 7 and 3 of the 8 bit input. Existing techniques use ROM for storing the predefined values or generate the values using Composite Field Arithmetic and the minimum slices reported by the existing techniques is 45 slices by the work of Bahram (2013). These techniques increased the delay and complexity respectively, and so cannot be used for small area applications. In the proposed architecture, use of inbuilt Mux reduced the area and the delay was reduced due to reduction in search space during SubByte transformation. The proposed Mux Based SBox occupied a lesser number of slices (Area: 40 Slices, Delay: 2.17 ns) when compared to other implementation techniques because of the use of MUX which are inbuilt in FPGA. A similar approach can be applied to MixColumn operations to reduce the computational complexity.
Mux Based MixColumn

Structural modifications were applied to another computationally intensive transformation of AES algorithm which is the MixColumn transformation. In this transformation, each column of the state array is multiplied by a predefined fixed polynomial. In the proposed structure, Multiplexers are used to select the column and the values with which it has to be multiplied. This technique also reduced the need for multipliers as only Shift and XOR operations were involved. Thus the proposed Mux Based MixColumn achieved low area and optimum delay compared to existing techniques (Area: 38 Slices, Delay: 2.72 ns). Among the existing techniques the minimum slices occupied was by the work of Solmaz (2009), which used 43 Slices to implement MixColumn transformation.

These modifications were implemented using VHDL on Virtex 6 FPGA. Simulation of the codes was done using ModelSim 6.5 and Synthesized in Xilinx 13.1. The results thus obtained were compared with the existing techniques available and it was found that the Mux based SBox and MixColumn occupied lesser number of slices. The proposed Mux based SBox and MixColumn can be involved in designing an efficient AES architecture by integrating with the proposed Folded PSP architecture for high throughput.

Design of Optimized AES Architectures

The third objective of this research work was to optimize the AES architecture which gives better efficiency in terms of Throughput / Slice. Detailed description and implementation results were discussed in Chapter 5. In this research work, two integrated architectures (InFo PSP and Compact AES) were designed by integrating the best throughput and low area architectures proposed in Chapter 3 and Chapter 4.
Integrated Folded PSP Architecture

In this proposed architecture, Mux Based SBox and Mux Based MixColumn were integrated with Folded PSP architecture to improve the overall performance of the InFo PSP. This architecture achieved the highest throughput and optimized area (Throughput: 80.9 Gbps, Area: Efficiency: 14.9 Mbps) when implemented on Virtex 6 FPGA. Folded PSP architecture can achieve higher throughput and the Mux based SBox and MixColumn reduced area and delay compared to existing techniques. Reduction in delay further increased the processing speed, thus the proposed InFo PSP achieves the highest throughput. Using an iterative structure in this architecture area can be reduced considerably.

Compact AES Architecture

Need for small cryptographic core in applications like wireless devices has led to the design of Compact AES architecture. In this proposed architecture, the Integrated Folded PSP (InFo PSP) architecture was looped to get the iterative structure which reduced the area. Overall efficiency (Throughput / Slice) of this architecture was improved because of the reduction in the number of slices occupied. (Throughput: 53.2 Gbps, Area: 1888 Slices, Efficiency: 28.1 Mbps). This optimized architecture can be used for high Throughput and low area based applications.

In this thesis, efficient and high performance implementation of AES algorithm is proposed and implemented. All the proposed architectures were implemented on Virtex-6 Device and Synthesized. The parameters were computed based on the synthesis reports generated. All the performance parameters are analyzed and compared with the existing techniques. The proposed AES architectures prove to be better than the existing architectures in terms of throughput and efficiency.
6.2 FUTURE SCOPE

This research work can be extended in many dimensions and are mentioned below.

✓ ASIC Based Implementation

Application Specific Integrated Circuits (ASIC) based implementation can be performed on the proposed architectures and accurate power consumed for a particular technology can also be computed.

✓ Intrusion Detection Schemes

Various attacks can be tried on the AES Algorithm by invasive and non invasive methods. A monitoring circuit can be designed which can detect and communicate any attacks on the Encryptor.

✓ Modes of Operations

Different modes of operations other than ECB mode can be applied to AES algorithm and a comparative study on the parameters can be made.