# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Title</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>DECLARATION</td>
<td>ii</td>
</tr>
<tr>
<td>BONAFIDE CERTIFICATE</td>
<td>iii</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENT</td>
<td>iv</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>v</td>
</tr>
<tr>
<td>TABLE OF CONTENTS</td>
<td>ix</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>xi</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td>xv</td>
</tr>
<tr>
<td>PRINCIPAL NOMENCLATURE</td>
<td>xvi</td>
</tr>
</tbody>
</table>

## 1 INTRODUCTION

1.1 Network Security                                        | 1        |
1.2 Cryptography in Network Security                        | 3        |
1.3 Requirements of Cryptographic Algorithms                | 4        |
1.4 Types of Cryptosystems                                  | 5        |
1.5 Implementation Platforms                               | 11       |
1.6 Research Challenges                                     | 16       |
1.7 Objectives of the Research                              | 17       |
1.8 Research Contributions                                  | 18       |
1.9 Thesis Outline                                          | 20       |
1.10 Summary                                                | 20       |

## 2 A REVIEW ON THE AES IMPLEMENTATION TECHNIQUES

2.1 Introduction to AES                                     | 22       |
2.2 Review of Architectural modifications on AES            | 25       |
2.2.1 Architectures for High Throughput                     | 26       |
# TABLE OF CONTENTS

2.2.2 Architectures for Low Area 34

2.3 Review of Structural Modifications on AES 39
  2.3.1 Architectures for SBox Implementations 39
  2.3.2 Architectures for MixColumn Implementations 49

2.4 Review of Other Optimization Techniques 51

2.5 Summary 58

3 PROPOSED AES ARCHITECTURES FOR HIGH THROUGHPUT 60
  3.1 Proposed Folded Parallel Architecture 62
  3.2 Proposed Parallel SubPipelined Architecture 75
  3.3 Proposed Folded Parallel SubPipelined Architecture 78

4 PROPOSED AES ARCHITECTURE FOR LOW AREA 86
  4.1 Proposed Multiplexer Based implementation of SBox 88
  4.2 Proposed Multiplexer Based implementation of MixColumn 95

5 PROPOSED AES ARCHITECTURES FOR HIGH EFFICIENCY 103
  5.1 Proposed Integrated Folded PSP Architecture 104
  5.2 Proposed Compact AES Architecture 110

6 CONCLUSION AND FUTURE SCOPE 119
  6.1 Summary 119
  6.2 Future Scope 125

REFERENCES 126

LIST OF PUBLICATIONS BASED ON THESIS 141

CURRICULUM VITAE 143