A Survey on Advanced Encryption Standard

Sandeep Kumar Rao¹, Dindayal Mahto², Dr. Danish Ali Khan³

¹, ², ³National Institute of Technology, Jamshedpur, India

Abstract: Rijndael’s Advanced Encryption Standard (AES) is the block cipher based symmetric-key cryptography to protect the sensitive information. The key sizes of AES are 128, 192, 256 bits. AES is based on substitution-permutation strategy. It is accepted by NIST in 2001 after the five year of security evaluation. It is highly secured and efficient than Data Encryption Standard (DES) and other symmetric-key cryptographic algorithms. This paper depicts all the valuable work done on the Advanced Encryption Standard since it is accepted by National Institute of Standards and Technology (NIST).

Keywords: AES, DES, Composite Field Arithmatic(CFA), Field Programmable Gate Array(FPGA), Correlation Power Analysis(CPA)

1. Introduction

In 1997, NIST wished to form a successor of DES after some security flaws in DES [3]. Two conferences were held (AES1 in August 1998 and AES2 in March 1999) and the motive was not only the security but also the performance in various aspects of settings [3]. In October 2000, Rijndael algorithm for encryption/decryption is selected and after the five years of long security and performance testing [4], is accepted by the U.S government in 2001.

The AES was published in 2001 by NIST as the symmetric block cipher algorithm and become the successor of DES as approved standard.

In AES, cipher takes block size of 128 bits for in both hardware and software implementation [5]. AES block size is fixed that is 128 bits and key sizes of 128,192 and 256 bits respectively but Rijndael’s block sizes and key sizes are multiple of 32 bits with a minimum of 128 bits [1].

The block sizes have a limitation of 256 bits but key sizes are not fixed theoretically.AES uses 128,192 and 256 bits key sizes and 10, 12 and 14 round respectively. There has been attack on 7 rounds for 128-bit, 8 rounds for 192-bit and 9 rounds for 256-bit keys[6].

AES is highly structured and efficient algorithm to protect the classified information at the highest secure level[7].

2. Structure of Advanced Encryption Standard

NIST accepted the AES as a Federal Information processing Standard (FIPS)-197. The 128 bits inputs are arranged in block of bytes using 4x4 square matrix. The bytes processing is defined in the Galois Field GF(2⁸). There are specified repeated steps involved in the each round of encryption and inverse steps are involved to getting back original plaintext[6,7].

The following steps involved in the encryption process:
1) Initial Round: AddRoundKey
2) Rounds: SubBytes, ShiftRows, MixColumns, and AddRoundKey
3) Last Round: SubBytes, ShiftRows, and AddRoundKey
3. AES Encryption and Decryption

a) AES most important feature is that it is not a Feistal structure. In Feistal structure half of the data block is used to modify the other half of data block and so then the half are swapped.

b) AES process the entire data block using a single square matrix during each round using substitutions and permutation.

c) The key is expanded into array of 44 (32-bit words), w_i.

d) Four steps are used, one of permutation and three of substitution

i) Substitute bytes

ii) ShiftRows

iii) MixColumns

iv) AddRound Key

Fig. 7 shows the overall encryption and decryption process.
4. S-Box Enhancement and Modification:

4.1 General Modification

a) Algebraic representation of Rijndael:
Rijndael block cipher uses the closed algebraic formulae that highly structured and very simple than any other algebraic formulation of block cipher that we know[8].

Rijndael S-Box can be written as an equation form that is

\[ S(x) = w_8 \sum_{d=0}^{7} w_d x^{255-2^d} \]

where \( w_8 \) is a constant and varies from \( w_0 \) to \( w_7 \).

Since in every round except last round, the output of S-Box is multiplied by Maximum Distance Separable (MDS) matrix and after that key is added.

Due to linearity of MDS matrix and key addition \( w_8 \) constant can be replaced by some constant.

Now the equation will be in the following form

\[ S(x) = \sum_{d=0}^{7} w_d x^{2^d} \]

here modified key schedule is used so it gives \( x^{255} = 1 \), except for all \( x = 0 \).

So the equation is simplified as

\[ S(x) = \sum_{d=0}^{7} w_d x^{2^d} \]

After byte substitution, ShiftRow operation, MixColumns, and key addition the equation is taken as:

\[ a_{i,j}^{(r+1)} = k_{i,j}^{(r)} + \sum_{e_d \in E} w_{i,e_d,i,j} x^{2^{e_d}} \]

\[ a_{i,j}^{(r+1)} = \text{byte at position } (i,j) \text{ at final round.} \]

\( k_{i,j}^{(r)} = \text{round key at position } (i,j). \)
\( e_d = \text{constant term in MixColumn step}. \)
\( d_r = \text{constant term in initial round}. \)
\( E = \{0, \ldots, 3\} \)
\( D = \{0, \ldots, 7\} \)

This algebraic representation for Rijndael still do not have any attack and it works properly.

b) S-Box Complexity

Rijndael’s S-Box is very simple and it involves only 9 terms without any particular reason. So it is taken as a open challenge.

AES S-Box complexity can be increased to 255 terms to increase high reliable security of AES[9].

After the improvement complexity can be increased from 9 to 255 terms. In this case complexity as well as security and performance of former algorithm is improved. Later algorithm is more resisting against the cryptanalysis attacks.

<table>
<thead>
<tr>
<th>F</th>
<th>E</th>
<th>D</th>
<th>C</th>
<th>B</th>
<th>A</th>
<th>9</th>
<th>8</th>
<th>7</th>
<th>6</th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>59</td>
<td>93</td>
<td>FD</td>
<td>92</td>
<td>CF</td>
<td>88</td>
<td>b1</td>
<td>8b</td>
<td>80</td>
<td>ab</td>
<td>ed</td>
<td>FF</td>
<td>15</td>
<td>96</td>
<td>ce</td>
</tr>
<tr>
<td>1</td>
<td>29</td>
<td>69</td>
<td>BF</td>
<td>59</td>
<td>21</td>
<td>C1</td>
<td>ec</td>
<td>37</td>
<td>91</td>
<td>c3</td>
<td>92</td>
<td>9b</td>
<td>6b</td>
<td>60</td>
<td>9a</td>
</tr>
<tr>
<td>2</td>
<td>3d</td>
<td>9a</td>
<td>f8</td>
<td>69</td>
<td>00</td>
<td>a4</td>
<td>f7</td>
<td>0b</td>
<td>89</td>
<td>b9</td>
<td>f7</td>
<td>88</td>
<td>4c</td>
<td>4a</td>
<td>59</td>
</tr>
<tr>
<td>3</td>
<td>22</td>
<td>4c</td>
<td>1c</td>
<td>3c</td>
<td>00</td>
<td>b9</td>
<td>37</td>
<td>2f</td>
<td>7e</td>
<td>ab</td>
<td>84</td>
<td>7d</td>
<td>67</td>
<td>9a</td>
<td>53</td>
</tr>
<tr>
<td>4</td>
<td>74</td>
<td>b1</td>
<td>2c</td>
<td>1c</td>
<td>77</td>
<td>f0</td>
<td>ef</td>
<td>7d</td>
<td>0e</td>
<td>7d</td>
<td>67</td>
<td>b9</td>
<td>21</td>
<td>b1</td>
<td>74</td>
</tr>
<tr>
<td>5</td>
<td>19</td>
<td>99</td>
<td>1e</td>
<td>4d</td>
<td>57</td>
<td>7c</td>
<td>6c</td>
<td>1e</td>
<td>nc</td>
<td>19</td>
<td>98</td>
<td>cf</td>
<td>bc</td>
<td>3c</td>
<td>42</td>
</tr>
<tr>
<td>6</td>
<td>9c</td>
<td>bc</td>
<td>h6</td>
<td>97</td>
<td>39</td>
<td>4f</td>
<td>f1</td>
<td>6d</td>
<td>5d</td>
<td>4e</td>
<td>9a</td>
<td>59</td>
<td>55</td>
<td>94</td>
<td>6b</td>
</tr>
<tr>
<td>7</td>
<td>4a</td>
<td>8d</td>
<td>55</td>
<td>74</td>
<td>f0</td>
<td>5c</td>
<td>93</td>
<td>2c</td>
<td>95</td>
<td>e5</td>
<td>8b</td>
<td>29</td>
<td>3e</td>
<td>5c</td>
<td>88</td>
</tr>
<tr>
<td>8</td>
<td>22</td>
<td>4c</td>
<td>1c</td>
<td>3c</td>
<td>00</td>
<td>b9</td>
<td>37</td>
<td>2f</td>
<td>7e</td>
<td>ab</td>
<td>84</td>
<td>7d</td>
<td>67</td>
<td>9a</td>
<td>53</td>
</tr>
<tr>
<td>9</td>
<td>d0</td>
<td>cf</td>
<td>65</td>
<td>21</td>
<td>22</td>
<td>90</td>
<td>f3</td>
<td>37</td>
<td>a8</td>
<td>8d</td>
<td>23</td>
<td>30</td>
<td>4d</td>
<td>6b</td>
<td>2e</td>
</tr>
<tr>
<td>10</td>
<td>28</td>
<td>8d</td>
<td>65</td>
<td>21</td>
<td>22</td>
<td>90</td>
<td>f3</td>
<td>37</td>
<td>a8</td>
<td>8d</td>
<td>23</td>
<td>30</td>
<td>4d</td>
<td>6b</td>
<td>2e</td>
</tr>
<tr>
<td>11</td>
<td>09</td>
<td>df</td>
<td>f0</td>
<td>1c</td>
<td>4c</td>
<td>55</td>
<td>74</td>
<td>f0</td>
<td>5c</td>
<td>93</td>
<td>2c</td>
<td>95</td>
<td>e5</td>
<td>8b</td>
<td>29</td>
</tr>
</tbody>
</table>

Figure 8: Improved AES S-Box

Substitute byte operation and its access time is fixed and indestructible. S-Box using combinational logic contains small area and it provides high level efficiency and throughput. In the combinational based S-Box stage pipeline is introduced for the S-Box implementation[10]. Area is taken by this design is 43 slices and maximum clock frequency of 72.155 MHZ.

Substitute byte transformation:
It is computed by taking the multiplicative inverse in GF(2^8) followed by Affine transformation of input byte.

Reverse Substitute transformation:
It is the reverse process of Substitute byte transformation. Reverse Substitute transformation is computed by applying inverse of Affine transformation followed by the taking the multiplicative inverse in GF(2^8).

<table>
<thead>
<tr>
<th>F</th>
<th>E</th>
<th>D</th>
<th>C</th>
<th>B</th>
<th>A</th>
<th>9</th>
<th>8</th>
<th>7</th>
<th>6</th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>59</td>
<td>93</td>
<td>FD</td>
<td>92</td>
<td>CF</td>
<td>88</td>
<td>b1</td>
<td>8b</td>
<td>80</td>
<td>ab</td>
<td>ed</td>
<td>FF</td>
<td>15</td>
<td>96</td>
<td>ce</td>
</tr>
<tr>
<td>1</td>
<td>29</td>
<td>69</td>
<td>BF</td>
<td>59</td>
<td>21</td>
<td>C1</td>
<td>ec</td>
<td>37</td>
<td>91</td>
<td>c3</td>
<td>92</td>
<td>9b</td>
<td>6b</td>
<td>60</td>
<td>9a</td>
</tr>
<tr>
<td>2</td>
<td>3d</td>
<td>9a</td>
<td>f8</td>
<td>69</td>
<td>00</td>
<td>a4</td>
<td>f7</td>
<td>0b</td>
<td>89</td>
<td>b9</td>
<td>f7</td>
<td>88</td>
<td>4c</td>
<td>4a</td>
<td>59</td>
</tr>
<tr>
<td>3</td>
<td>22</td>
<td>4c</td>
<td>1c</td>
<td>3c</td>
<td>00</td>
<td>b9</td>
<td>37</td>
<td>2f</td>
<td>7e</td>
<td>ab</td>
<td>84</td>
<td>7d</td>
<td>67</td>
<td>9a</td>
<td>53</td>
</tr>
<tr>
<td>4</td>
<td>74</td>
<td>b1</td>
<td>2c</td>
<td>1c</td>
<td>77</td>
<td>f0</td>
<td>ef</td>
<td>7d</td>
<td>0e</td>
<td>7d</td>
<td>67</td>
<td>b9</td>
<td>21</td>
<td>b1</td>
<td>74</td>
</tr>
<tr>
<td>5</td>
<td>19</td>
<td>99</td>
<td>1e</td>
<td>4d</td>
<td>57</td>
<td>7c</td>
<td>6c</td>
<td>1e</td>
<td>nc</td>
<td>19</td>
<td>98</td>
<td>cf</td>
<td>bc</td>
<td>3c</td>
<td>42</td>
</tr>
<tr>
<td>6</td>
<td>9c</td>
<td>bc</td>
<td>h6</td>
<td>97</td>
<td>39</td>
<td>4f</td>
<td>f1</td>
<td>6d</td>
<td>5d</td>
<td>4e</td>
<td>9a</td>
<td>59</td>
<td>55</td>
<td>94</td>
<td>6b</td>
</tr>
<tr>
<td>7</td>
<td>4a</td>
<td>8d</td>
<td>55</td>
<td>74</td>
<td>f0</td>
<td>5c</td>
<td>93</td>
<td>2c</td>
<td>95</td>
<td>e5</td>
<td>8b</td>
<td>29</td>
<td>3e</td>
<td>5c</td>
<td>88</td>
</tr>
<tr>
<td>8</td>
<td>22</td>
<td>4c</td>
<td>1c</td>
<td>3c</td>
<td>00</td>
<td>b9</td>
<td>37</td>
<td>2f</td>
<td>7e</td>
<td>ab</td>
<td>84</td>
<td>7d</td>
<td>67</td>
<td>9a</td>
<td>53</td>
</tr>
<tr>
<td>9</td>
<td>d0</td>
<td>cf</td>
<td>65</td>
<td>21</td>
<td>22</td>
<td>90</td>
<td>f3</td>
<td>37</td>
<td>a8</td>
<td>8d</td>
<td>23</td>
<td>30</td>
<td>4d</td>
<td>6b</td>
<td>2e</td>
</tr>
<tr>
<td>10</td>
<td>28</td>
<td>8d</td>
<td>65</td>
<td>21</td>
<td>22</td>
<td>90</td>
<td>f3</td>
<td>37</td>
<td>a8</td>
<td>8d</td>
<td>23</td>
<td>30</td>
<td>4d</td>
<td>6b</td>
<td>2e</td>
</tr>
<tr>
<td>11</td>
<td>09</td>
<td>df</td>
<td>f0</td>
<td>1c</td>
<td>4c</td>
<td>55</td>
<td>74</td>
<td>f0</td>
<td>5c</td>
<td>93</td>
<td>2c</td>
<td>95</td>
<td>e5</td>
<td>8b</td>
<td>29</td>
</tr>
</tbody>
</table>

Figure 9: Coefficient of New(improved) AES S-Box

There is relation between data and its correspondence
Coefficient in improved AES S-Box.

4c 88 6b 60 9b 9a 6b 9a 9b 6b 60 9a af

- c) S-Box based on combinational logic
Affine Transformation

Volume 6 Issue 1, January 2017
Inverse-Affine Transformation:
\[
\begin{pmatrix}
\text{b}_0 \\
\text{b}_1 \\
\text{b}_2 \\
\text{b}_3 \\
\text{b}_4 \\
\text{b}_5 \\
\text{b}_6 \\
\text{b}_7
\end{pmatrix}
= \begin{pmatrix}
1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}
\begin{pmatrix}
\text{b}_0 \\
\text{b}_1 \\
\text{b}_2 \\
\text{b}_3 \\
\text{b}_4 \\
\text{b}_5 \\
\text{b}_6 \\
\text{b}_7
\end{pmatrix}
\]

Note: S-Box can be generated by replacing the Affine Transformation matrix.

Here we can see that both SubByte and inverse SubByte contain a multiplicative inversion operation. Both involves the same multiplicative inversion operation in combined manner. Due to the similarity of SubByte and inverse SubByte than their operation followed by Affine transformation and its inverse, only implementation of SubByte is essential.

de) S-Box rotation

AES can be enhanced in security by applying the key dependent AES using S-box rotation[11]. In this algorithm, Key expansion along with S-box rotation makes the S-Box key dependent. This approach of key dependent S-box is much harder for attackers in doing any analysis.

Fig.10 depicts the New planned key dependent Encryption.

![Figure 10: A new approach for key dependent Encryption](image)

Fig.11 shows the Decryption for newly proposed key dependent S-Box.

Round key is generated in each round using cipher key with the help of key scheduling algorithm.

e) S-Box construction

S-Box is the backbone of AES encryption standard. Rijndael’s S-Box is created by the first irreducible polynomial out of thirty irreducible polynomial that can be constructed of the same degree over GF(2^8). The isomorphic field to the core field can be generated by using differential irreducible polynomial of same degree over GF(2^8)[12].

Irreducible polynomial can be made by following Mobius function i.e
\[
\sum_{d|n} \mu(d) \cdot p^{n/d}, \text{ where } \mu \text{ is Mobius Function}
\]
\[
\mu(n) =
\begin{cases} 
0 & \text{if } n=1 \text{ or more prime factor} \\
1 & \text{if } n=1 \\
(-1)^k, \text{ n=product of k distinct primes}
\end{cases}
\]

from above equation a total of 30 irreducible polynomial of same degree(8) over GF(2^8) can be generated. Irreducible polynomial that is used in AES originally is \((x^8 + x^4 + x^3 + x + 1)\).

Some polynomials are listed below i.e
\[
1) \ x^8+x^4+x^3+x+1 \\
2) \ x^8+x^5+x^4+x+1 \\
3) \ x^8+x^4+x^3+1 \\
4) \ x^8+x^4+x^3+x^2+1 \\
5) \ x^8+x^4+x^3+x+1 \\
6) \ x^8+x^4+x+1 \\
7) \ x^8+x^4+x^3+1 \\
8) \ x^8+x^4+x^3+x^2+1 \\
9) \ x^8+x^4+x^3+x^2+1 \\
10) \ x^8+x^4+x^3+x^2+1 \text{ etc.}
\]

Affine matrix:

Affine matrix can also be made that can replace the existing affine matrix and still this matrix works in efficient way. Affine matrix \(A \in \text{GL(2^n)}\), it is a general linear group of degree 8 over the Galois Field,GF(2) and the group order is

\[
\prod_{k=0}^{7} (2^8 - 2^k) \approx 5.3481 \times 10^{18}
\]
using above equation we can generate numerous Affine matrix. This is well tested on MAT Lab.

Some affine matrix are shown below

\[
\begin{bmatrix}
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 1
\end{bmatrix}
\]

4.2 Hardware based design for S-Box

a) Compact and High speed hardware design for Rijndael algorithm

Rijndael’s algorithm can also be implemented on hardware with high efficiency and speed[13].

S-Box can be optimized by using composite field.

In Encryption and decryption all the arithmetic components are reused and data path is combined.

It can be obtained of enormously small size 5.4Kgates for 128-bit key Rijndael’s circuit by means of 0.11µm CMOS standard.

Cell library.

It occupies only 0.052mm² area for both encryption/decryption with 311 mbps throughput. It can be increased upto 2.6Gbps of size 21.3Kgates for high speed implementation.

In hardware approach both Encryption/Decryption block uses 16-byte data register and ShiftRow operation or Inverse-ShiftRow processed by self.

In this approach Shiftrow(or Inverse-ShiftRow) and SubByte(or Inverse-SubByte) is different but there is no any effect on this algorithm, it works properly.

S-Box is used only once in Key Expansion and 4-times used in Both Encryption and Decryption block

During Key Expansion S-Box and ShiftRow (or Inverse-ShiftRow ) operationsare executed simultaneously. Initial round requires 4-cycle because there is no S-Box transformation is needed and remaining round takes 5-cycles.

Total of (4+5*10)=54cycles needed.

b) Multiplexer-Look-Up-Table(MLUT)based S-Box

To protect the AES from side channel attacks(SDAs), MLUT can be used as a countermeasure against SDAs[18]. It requires 256-bytes to 1-byte multiplexer and memory uses 256 bytes[19]. Multiplexer based S-Box is 30 times more secure regarding SDAs than conventional AES based.

Secret information can be leaked by correlating its transitional data with leaked physical parameter. Leaked physical elements can be power dissipation, electromagnetic radiation, and timestamp information.

SDA can be analyzed by three way:
- Simple Power Analysis(SPA)
- Differential Power Analysis(DPA)
- Correlation Power Analysis(CPA)

CPA is the powerful attack than other. Basically two countermeasure can be applied on CPA[18] i.e
- Hiding (hardware based)
- Masking (software based)

In hiding technique, the dependency between transitional data and physical elements is being reduced. In masking transitional data is being masked for securing against leaked elements.
c) S-Box over Composite Field Arithmetic (CFA)
As we have seen that S-Box is made over the GF(2^8).
Decomposition of GF(2^8) into GF(((2^2)^2)^2) provides another way of making S-Box.

Implementation of CFA on Field Programmable gate Array (FPGA) reduces the gates count that is used in hardware than the conventional Look Table based S-Box.

S-Box, based on CFA on hardware reduces the area by 50% and also diminishes the power consumption.

This architecture replaces the conventional S-Box based on look Up table to Composite Field Arithmetic design.

Using CFA, S-Box can be constructed in 16 different proposed ways[14].
GF(2^8) can be decomposed into GF((2^3)^2) and GF((2^3)^2). GF(2^8) to GF(((2^3)^2)^2), a total of eight isomorphic mapping elements can be constructed.

S-Box can be shown as
S=MS^{-1}+C

Here multiplicative inversion over GF(2^8) is followed by Affine transformation matrix.
M=8x8 binary matrix
C=8-bit binary vector
CFA that contains irreducible polynomial

Can be represented as:
GF(2^8):x^8+x+1
GF((2^3)^2):x^2+x+\phi, \phi=[10]_2
GF(((2^3)^2)^2):x^2+x+\lambda, \lambda=[1100]_2

For \phi=[10]_2, \lambda=[1100]_2 smallest amount of gate count in hardware and low power consumption can be seen.

d) Gray S-Box
Binary gray encoding technique can be a better option for increasing the complexity of algebraic expression[15]. It provides a easiest implementation in digital communication systems. Gray code is an encoding technique by a single bit difference for the consecutive value.

Binary gray code can be calculated as

For a=[0 to n], input array in binary form,
  b=[0 to n], output array in binary form,
where [0] is LSB.

b[n] =a[n];
for k = (n-1) to 0
b[k] =a[k+1] \oplus a[k].

In GF(2^5) binary number can be converted into linear form as

\[
\begin{bmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 \\
\end{bmatrix} \times \begin{bmatrix}
a_0 \\
a_1 \\
a_2 \\
a_3 \\
a_4 \\
a_5 \\
\end{bmatrix} = \begin{bmatrix}
a_0 \\
a_1 \\
a_2 \\
a_3 \\
a_4 \\
a_5 \\
\end{bmatrix}
\]

where (a_0 is the LSB bit), and a_i is the k^{th} bit of byte a.
b_i = k^{th} bit of byte b.

Let a=x and b=y;

AES polynomial in GF(2^5)[x]/(m(x)) can be represented in linear form as
L(x) = \text{8f}x^{(7f)}+\text{b5}x^{(bf)}+\text{01}x^{(df)}+\text{f4}x^{(ef)}+\text{25}x^{(f7)}+\text{f9}x^{(7b)}+\text{09}x^{(7d)}+\text{05}x^{(7e)}+\text{63}

Above expression can be replace by gray code conversion as
G(x)=(98)x^{(80)}+(e5)x^{(40)}+(4e)x^{(20)}+(3c)x^{(20)}+(13)x^{(08)}+(93)x^{(04)}+(9b)x^{(02)}+(15)x

The modified S-Box or Gray S-Box can be given as amalgamation of original AES and Gray code conversion G(x).

Gray S-Box can be represented as function as follow
G_s(x)=\sum_{i=0,j=0}^{15} a_{ij} x^{16i+j}

where a_{ij} is hexadecimal value in i^{th} row and j^{th} column given in Fig.17

Here the highest degree of algebraic expression is 254 and total of 255 terms than original AES which has only 9-terms.

Inverse Gray S-Box function can be given as
G_s^{-1}(x)=\sum_{i=0,j=0}^{15} b_{ij} x^{16i+j}

where b_{ij} is hexadecimal value in i^{th} row and j^{th} column given in Fig.18.
Gray S-Box has some properties:
   a) Non-Linearity
   b) Differential equality
   c) Strict avalanche standard

Further it provides security from different algebraic attack and interpolation attack.

4.3 S-Box using Genetic Algorithm and Neural network

In AES cryptosystem, a greater complexity leads to a greater security to resisting any cryptanalytic attacks. But increasing complexity leads to increasing in processing time and can get timing attacks. In this situation Genetic Algorithm (GN) and Neural Network (NN) can be better option for reducing the processing time and provides security from timing attacks[16].

As we know that AES is based on Substitution-permutation based encryption system.

In GA and NN system, as a Substitution-permutation Network (SPN) it provides the non-linearity to the system and resistance to the cryptanalytic attacks.

Genetic Algorithm:
Genetic Algorithm is basically used for substitution and some transposition [54]. It creates cipher for block and generates keys[55] and also is used for both text and images. It uses basically three operators

a) Selection: selection of chromosomes that is generated by Pseudo Random Number Generator (PRNG) on initial population.
   b) Crossover: to reproduce a new set of values by combining one generated chromosome with another.
   c) Mutation: it is used for presenting difference of chromosomes that is newly generated.

Figure 17: Gray S-Box

Figure 18: Inverse S-Box

Figure 19: Genetic Algorithm working manner

Figure 20: Functioning of AES with GA

Figure 21: Architecture of Neural Network
4.4 Cellular Automata based S-Box

Cellular Automata’s concept was come in 1940 that was given by von Neumann and Ulam to learn the idea of biological process i.e Self-reproduction [17].

It has the property of parallel processing so implementation speed is high compared with classical AES S-Box.

In CA’s system, space and time are distinct. It’s basically used for creating a pseudo random number.

It is an array of cells and at particular time state of a cell is determined by the current states of neighborhood cells.

In CA array of cell is n-dimensional and the identical rule that is enclosed in every cell is a finite state machine and it can be precise in rule table (or transition function).

Rule table contains an entry to every neighborhood relationship of states.

In 1-D CA, a cell contains r local neighbor at either side and to itself also where r is the radius so it make total of (2r+1) neighbors.

5. FPGA Implementation of AES

As we know that Rijndael’s AES encryption/decryption algorithm is selected after the proper implementation on software as well as hardware. For hardware implementation, Field Programmable Gate Array (FPGA) become the more suitable option. It is reprogrammable device that provides agility, physical security and high performance than any software implementation [20].

FPGA specification is given in [21].

FPGA mainly focus on three area:
  a) Algorithm integrity
     • It ensures the originality of data at any instant of time[22].
  b) High throughput
     • It ensures the encryption as fast as possible [23,24].
  c) Low power consumption
     • It ensures the lower consumption of Power [25,26].

By means of power analysis, normal AES is broken in 1999 [56]. To protect the data from differential power analysis (DPA) attacks, a high throughput masked AES is projected [57]. In AES block cipher Power and Sizes can also be reduced by using compact key expansion mechanism. It can be design with mainly three methodologies:

  • Implementation of optimized number of AES S-Box [27]
  • Dipping down the number of pipeline register
  • Sharing input bus

It gives three optimized architecture. Total of 1818 logic element, 122.04mW power dissipation and throughput of 198.77Mbps is obtained in best architecture [28].
6. Design Technique of AES regarding Complexity

6.1 Area efficient and Low-Cost Design of AES

[29] An Area-Efficient design of Advanced Encryption Standard (AES) can be made by eliminating the common sub-expression. As we know that in decryption, four Inverse transformation is performed i.e Inv-SubBytes (ISB), Inv-ShiftRows (ISR), Inv-MixColumns (IMC) and AddRoundKey.

Since decryption process by swapping of ISR and ISB is not affected and IMC can also be processed before ARK as long as the round key in the ARK undergo IMC function.

After performing this swapping, decryption process become equivalent to the encryption process regarding sequence of transformation except for inverse transformation and modified key expansion.

Figure 25: Equivalence of encryption and modified Decryption regarding sequence of transformation.

To design a low complexity AES, a method of using extended instruction technique can be used in which the instructions is reduced from 688 to 340 [30].

6.2 High Regular and Scalable AES Architecture

AES hardware based design can be made as a high regular and scalable. it can present a high throughput of 241 Mbits/s on a 0.6 µm area of CMOS process [36].

Figure 26: Hardware Module of the AES

This Hardware Module contains four components i.e Interface
It handles all the communication of this module with its surroundings and it’s communication is based on 32-bit data words.

6.3 Pipelined Architecture of AES

Two architecture can be used for Encryption/Decryption. First Architecture can be based on feedback strategy and can reach to throughput value of 259Mbit/s. Second Architecture is based on Pipeline technique and can reach to throughput value of 3.65Gbit/s. Second Architecture has two characteristics:

a) Pipeline Technique
b) Key Storage using RAM.

Pipeline Technique can not possible for other cryptographic application but Rijndael’s AES can be implemented using pipeline technique, paper [60] can be referenced for more details.

Hardware implementation provides high throughput than software implementation [59].

AES can be implemented on parallel, pipeline and in sequential manner. The Field Programming Gate Array (FPGA) is used for performing parallel operations. Throughput can be increased to three times after using these three implementation of AES [58].

6.4 Dual Core Architecture

A Dual Core architecture is described in paper [31]. In compact Dual-Core Architecture, encryption and decryption is done simultaneously. it is used in real-time dual-duplex wireless communication. It uses 32-bit data path with four clock cycle to implement 128-bit data for one round.

Figure 27: Data path for encryption
6.5 Implementation on Grain on Sand

AES can be implemented on hardware which requires very less resources. It is implemented on 0.35µm CMOS process which requires only 0.25mm$^2$ area and needed 3400 gates that is corresponding to a size of a grain of sand. This is done on a semiconductor (i.e silicon) and called silicon implementation. It requires very less amount of hardware resources and the power efficiency is very high. Detailed description is given in paper [32].

7. Attacks and Countermeasure (if possible)

a) In [33], a parity based technique is given for error detection. Parity based concurrent checking method leads to hardware overhead because it adds one additional bit per bytes in 128-bit data. This result in 16 extra bits which modifies (8-bit × 8-bit) S-Box into (9-bit × 9-bit) S-Box.

To overcome the overhead due to the parity based concurrent checking, paper [34] describes the low-cost concurrent checking method.

This method checks for Substitution-Permutation-Network (SPN) and the input parity bit is modified according to the execution step of SPN into the output parity bit and then it is compared with output parity of every round.

b) Some attack is based on fault injection into the cryptographic devices which aim is to incorporating an error to recover the secret keys.

In taking countermeasure, an extension [35] is done on an existing AES architecture which is given by Mangard et al. [36].

A fault injection attack can be done on smart card implementing the AES.

In the countermeasure, paper [37] shows the technique to protect from this attack.

This attack can be a side channel attack known as Differential Fault Analysis and it uses the nonlinear robust error detecting codes to handle this attacks.

A high efficient fault can be induced in the AES round. It changes the mapping relationship of S-Boxes. Using this two fault models can be presented.

First model requires only 16 faulty ciphertexts to obtain the secret key of 128bit and second model requires two rounds attack by Differential Fault Analysis to achieve 4-byte round key in 9th round [38].

A Differential Fault Analysis attack can be done on during key expansion [39]. It can be seen in AES-128 with two faults, AES-192 with six and AES-256 with four faults using a new differential attack [40].

B. Baharak [40] proposed a impossible differential attack, which is done on AES-128 upto seven round. It requires $2^{15.5}$ plaintext, $2^{109}$ bytes memory and $2^{19}$ seven round encryption. This impossible differential attack take advantage of differences that is impossible at several intermediate state of algorithm. [41] A Fault Round Modification analysis is developed, which can analyze the modification in AES round. This is efficient than Differential Fault Analysis.

c) [42] There can be a collision attack on the 7-round of Rijndael’s algorithm

It takes advantage of some collision that exist between the partial function bring by the cipher. Paper [43] describes the collision timing attacks. Since timing attributes on combination circuit depends on the I/O variation of function. This characteristic can be gain by fault sensitivity analysis.

Due to the access time uncertainty and resource sharing in cache memory, there has been a timing attack which can leak secret information.

To find full AES keys, first round takes 300 samples and second round takes 80 samples [44].

[45] To prevent AES algorithm from Differential Power Analysis (DPA) , masking of logical gates is very effective. In spite of this masking, logic circuit used in implementation of AES algorithm, leak the side channel secret information which can be taken advantages in Differential power attacks.

A clock wise collision attack can also be induced in masked AES. It is also known as Fault Rate Analysis. In this attack, clock glitch is inject into the masked S-Box to recover the secret key [46].

A Low complexity attack can be done on AES upto four round using three known plaintext and it can also increased to six round [47].

8. Application of AES

8.1 Implementation in Smart card

In spite of three times faster than DES, AES is difficult to implement in smart card.

NexCard which is a Chip operating System, design by Microsoft, become the more suitable platform for implementing the AES as a efficient memory usage.
Cipher System on Demand (CSOD) method, utilizes the multi-application capacity of NexCard v2.0 to execute the same AES algorithm on Card [48]. In paper [49], also given integrated design of AES that gives the suitable hardware architecture to implement AES in smart card.

**8.2 AES in Radio Frequency Identification (RFID)**

AES can be used as a strong authentication in RFID. In this approach 128-bit data block uses 1000 clock cycles and power consumption is less than 9µA on 0.35µm CMOS[50].

![Figure 29: Structure of RFID](image)

**8.3 Image Encryption**

In today’s communication system, it is important to secure text data as well as multimedia data like image, video, audio etc. A modified AES can be made to fulfill this requirement.

In this version of AES, modification is focused on the ShiftRows transformations. The 1st and 4th row is unchanged when the value of 1st row and 1st column is even and the bytes of 2 and 3 rows is shifted right by different number.

Contrary, if first row and first column is odd, 1st and 3rd rows are unchanged and the byte of 2nd and 4th shifted left by different number[51].

AES can also be used to secure the biometric image data[52]. By using Singular Value Decomposition (SVD) and Discrete Wavelet Transform (DWT) as a SVD-DWT watermarking technique, AES can be use to transfer medical image securely[53].

**8.4 AES implementation for SANs**

To secure the large-scale Storage Area Network, AES can be used as trusted Encryption/Decryption Algorithm. It can be designed based on FPGA and takes advantage of all the resources of recent FPGA i.e Block RAM(BRAM) and Digital Signal Processing (DSP) slices[61].

**9. Performance of AES**

Now, it can said that AES works properly on software as well as hardware architecture. In hardware, it provides high performance from 8-bit processor to high bit processor. It provides throughput of 11Mb/s for a 200Mhz processor with a 18 clock cycles on a Pentium and a throughput of 60Mb/s on 1.7Ghz Pentium M processor[62].

![Figure 30: Comparison of AES with other cryptographic algorithm](image)

**10. Conclusion and Future Work**

Consequently it can be said that Rijndael’s AES Encryption/Decryption algorithm is high efficient and secure in terms of speed, time, throughput to any other symmetric cryptographic algorithm. It is very strong against different type of attacks like differential attacks, interpolation and square attack. This paper’s motive is to present all the valuable work that has been done on AES. Since increasing complexity leads to more security.

Hence, in future work our motive will be to test different S-Box in each round of Encryption / Decryption in which S-Boxes can be made by different polynomial of same degree i.e Galois Field ($2^8$).

**References**

Advanced encryption standard.


723


