Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

Survey and comprehensive Analysis for performance improvement of AES Encryption

Ashutosh Pandey[1], Umesh kumar[2], Sitendra Tamarkar[3]
[1]M.Tech Scholar, NIIST Bhopal, [2,3]A.P Dept. of CSE,NIIST Bhopal

Abstract—Now a day's it's a key challenge in data transmission to transfer data securely and efficiently. Cryptography techniques are widely use for secure data transmission over the communication network. Cryptography techniques are based on symmetric or asymmetric key based encryption. In Symmetric key based encryption and decryption process same key is use, also called private key. Advance encryption standard (AES) is one of the most popular and widely used symmetric encryption methods.AES is widely used by processor for secure and fast transmission of data. Performances and efficiency of AES processors are outstanding. For performance improvement of processors, efficiency with high throughput and fast processing in less encryption time are new challenges for researcher. Performance and security of AES algorithm is based on size of key and S-box. In this research paper we are presenting survey and comprehensive analysis for performance of different AES encryption with various key sizes. Existing AES use an S-Box with key size 128,192 and 256 bit.AES can be improved in terms of encryption time and speed and also decryption time and speed. Proposed IAES processor will perform outstanding over existing AES.

Keywords—AES, IAES Encryption, Decryption, S-box, Multistage S-box and Key

I. INTRODUCTION

The Advanced Encryption Standard (AES), the symmetric block cipher ratified as a standard by National Institute of Standards and Technology of the United States (NIST), this process helped to increase confidence in the security of the winning algorithm from those who were suspicious of backdoors in the predecessor DES.A new standard was needed primarily because DES has a relatively small 56-bit key which was becoming vulnerable to brute force attacks. In addition, the DES was designed primarily for hardware and is relatively slow when implemented in software [7]. While Triple DES avoids the problem of a small key size, it is very slow even in hardware; it is unsuitable for limited-resource platforms; and it may be affected by potential security issues connected with the (today comparatively small) block size of 64 bits. The AES is federal Information Processing Standard, (FIPS), which is a cryptographic algorithm that is used to protect electronic data [11, 13]. The AES algorithm is a symmetric block cipher that can encrypt and

decrypt information. Encryption converts data to an unintelligible form called cipher-text. Decryption of the cipher-text converts the data back into its original form, which is also called a Plain text [1].Cryptography plays an important role in the security of data. It enables us to store sensitive information or transmit it across insecure networks so that unauthorized persons cannot read it[14].

The urgency for secure exchange of digital data resulted in large quantities of different encryption algorithms which can be classified into two groups: asymmetric encryption algorithms (with public key algorithms) and symmetric encryption algorithms (with private key algorithms). Symmetric key algorithms are in general much faster to execute electronically than asymmetric key algorithms. The algorithm is composed of three main parts: Cipher, Inverse Cipher and Key Expansion[13]. Cipher

converts data to an unintelligible form called cipher text while Inverse Cipher converts data back into its original form called plaintext. Key Expansion generates a Key Schedule that is used in Cipher and Inverse Cipher procedure. Cipher and Inverse Cipher are composed of specific number of rounds [3]. For the AES algorithm, the number of rounds to be performed during the execution of the algorithm is dependent on the key length[15].

The Key Expansion step is performed using key schedule. The Initial Round consists only of an Add Round Key operation. The Rounds step consists of a Sub Bytes, Shift Rows, Mix Columns, and an Add Round Key operation. The number of rounds in the Rounds step varies from 10 to 14 depending on the key size. Finally, the Final Round performs a Sub Bytes, Shift Rows, and Add Round Key operations.

Decryption in AES is done by performing the inverse operations of the simple operations in reverse order. However, as shown later on in this paper, because of the block cipher mode of operation used, decryption is implemented but never used [9].

A. Encryption Process: The Encryption and decryption process consists of a number of different transformations applied consecutively over the data block bits, in a fixed number of iterations, called rounds. The number of rounds depends on the length of the key used for the encryption process. The four different transformations are described in detail below:

1) **Sub Bytes Transformation:** It is a non linear substitution of bytes that operates independently on each byte of the State using a substitution table (S box

2) **Shift Rows Transformation:** Shift rows transformation cyclically shifts the rows of the State over different offsets. The operation is almost the same in the decryption process except for the fact that the shifting offsets have different values.

3) **Mix Columns Transformation:** This is base and operates on the State column by column, treating each column as a four term polynomial. It also mixes columns results.

4) **Add Round Key Transformation:** In this transformation, a Round Key is added to the State by a simple bitwise XOR operation. Each Round Key consists of Nb words from the key expansion. Those Nb words are each added into the columns of the State. Key Addition is the same for the decryption process.

5) **Key Expansion:** Each round key is a four word (128-bit) array generated as a product of the previous round key, a constant that changes each round, and a series of S-Box lookups for each 32-bit word of the key.

B. AES Decryption Process: For decryption, the same process occurs simply in reverse order taking the 128-bit block of cipher text and converting it to plaintext by the application of the inverse of the four operations. Add Round Key is the same for both encryption and decryption.

However the three other functions have inverses used in the decryption process: Inverse Sub Bytes, Inverse Shift Rows, and Inverse Mix Columns. This process is direct inverse of the Encryption process. All the transformations applied in Encryption process are inversely applied to this process. Hence the last round values of both the data and key are first round inputs for the Decryption process and follows in decreasing order.

II. LITERATURE SURVEY

Authors [1] presented the design of an awfully low power and high throughput AES processor. A complicated AES algorithmic program while not sacrificing its safety features, throughput and space is used to design the processor. As a result of the optimization of the algorithmic program and variety of design issues, the processor shows its superiority over different AES processors. The proposed processor is simulated on the FPGA platform and Quartus II development software package of Altera device of family Stratix II GX is used to simulate the design.

An influence Play Early Power Estimation Tool is used to approximate the power consumption of the proposed processor. In a while the additional reliable power analysis tool named power play Power analyzer is employed to estimate the static and dynamic power dissipation within the Processor. The high level of system integration beside very low power consumption and high throughput makes the AES processor a perfect alternative for a spread of application as well as small computing devices, smart card readers and network applications like LAN, WPAN, and WSN etc.

Here author investigates the AES algorithm with relevancy FPGA and therefore the terribly High Speed integrated circuit Hardware Description language (VHDL). Software package is employed for simulation and improvement of the synthesizable VHDL code. All the transformations of each Encryptions and decryption are simulated victimization and reiterative design approach in order to minimize the hardware consumption. The Advanced encryption customary is programmed in software package or designed with pure hardware. But Field Programmable Gate Arrays (FPGAs) provide a faster, additional customizable answer.

Authors [2] presented an efficient and improved FPGA implementation of 128 bit block and 128 bit key AES cryptosystem has been bestowed during this paper. Optimized and Synthesizable VHDL code is developed for the implementation of each 128 bit data encryption and decryption method & description is verified victimization ISE 8.1 functional machine from Xillinx. All the transformations of algorithm are simulated victimization an iterative style approach in order to attenuate the hardware consumption. Every program is tested with a number of the sample vectors provided by NIST. The throughput reaches the worth of 352Mbit/sec for each encryption and decryption method with Device XCV600 of Xilinx Virtex Family.

Authors [3] proposed a configurable AES processor for extended security communication. The proposed design will provide up to 219 totally different AES block cipher schemes inside an affordable hardware cost. Data will be encrypted not solely with secret keys and initial vectors, however additionally by different block ciphers throughout the communication. A unique new concept of on the fly key growth style is additionally projected for 128-, 192-, and 256-bit keys. Our unified hardware will run the original AES algorithm and also the extended AES algorithm.

Authors [4] presented the implementation of the advanced standard and experience (AES) formula. They have used 128 bit block size and 128 bit cipher key for the execution. The AES conjointly called Rijndael algorithm is used to confirm security of communication channels. Xilinx design tool 13.3 and Xilinx project navigator design tool are used for synthesis and simulation. Very high speed integrated circuit hardware description language (VHDL) is used for coding. The absolutely pipelined style was enforced on vertex 6 FPGA family and a throughput of 49.3Gbits/s was achieved with and experience operational frequency of 384.793 MHz.

Authors [5] presented improve security against attack. The randomness of the S-Box is increase the avalanche effect and also increase the immunity power against attack compare to basic AES algo. For improving the security they propose the new approach in byte substitution round which uses two S-boxes alternatively for consecutive rounds. In the world of cryptography Advanced Encryption

Standard (AES) is one of the best algorithms of symmetric encryption technology. A new version of AES proposed in which two consecutive rounds of encryption and decryption uses two different s-boxes alternatively. The result of this process is the high bit independent criteria so the avalanche effect also increases. We have improved the security of AES by improving the avalanche criteria.

Authors [6] developed a more powerful algorithm for cryptography. This algorithm is based on AES to generate different sub key from the original key and using each sub key to encrypt one AES block. They used AES to protect our design from structural analysis, because AES is very resist modern attacks from other side generating many key from symmetric key resist modern attacks on symmetric key cryptography.

In this paper author [7] a detailed analysis of symmetric block encryption algorithms is presented on the basis of different parameters. The main objective was to analyze the performance of the most popular symmetric key algorithms in terms of Authentication, Flexibility, Reliability, Robustness, Scalability, Security, and to highlight the major weakness of the mentioned algorithms, making each algorithm's strength and limitation transparent for application. During this analysis it was observed that AES (Rijndael) was the best among all in terms of Security, Flexibility, Memory usage, and Encryption performance.

In this research paper [8] author proposed a HD cipher that securely encrypts a 128 bit counter value to a larger key brook. Replacing the AES used in CCMP with the HD cipher allows to achieving higher encryption throughput. Energy analysis experiments reveal that, HD cipher consumes 25% less energy compared to the traditional AES. Also, the proposed system performs significantly better when larger frame lengths are used.

III. PROBLEM STATEMEN

As the clock signal 'clk' corresponds to the data path of the encryption process, the speed performance is determined on the basis of this clock signal. So the speed of the crypto processor is also not well. Because the rounds step consists of a Sub Bytes, Shift Rows, Mix Columns, and an Add Round Key operation.

The number of rounds in the Rounds step varies from 10 to 14 depending on the key size, repeated for every 128 bit block and next block will be wait when previous block will be not complete the whole round step. Based on survey following key challenges are found for research and improvement in existing AES algorithm are-

1. **High encryption time**-Existing AES have high encryption time.
2. **High the decryption time**-Existing AES have high decryption time.
3. **Slow Encryption Speed**- Existing AES have low encryption speed.
4. **Slow Decryption Speed**- Existing AES have low decryption time.

IV. PROPOSED METHODOLOGY

In the proposed approach, the composite field S-box and inverse S-box are divided into blocks and the predicted parities of these blocks are obtained. Through exhaustive searches among all available composite fields, we find the optimum solutions for the least overhead parity based fault detection structures. Moreover, through our error injection simulations for one S-box (resp. inverse S-box),

We show that the total error coverage of 99.998% for 16 S-boxes (resp. inverse S-boxes) can be achieved. Finally, it is shown that both the ASIC and FPGA implementations of the IAES structures

using the obtained optimum composite fields, have better hardware and time complexities compared to their counter parts.

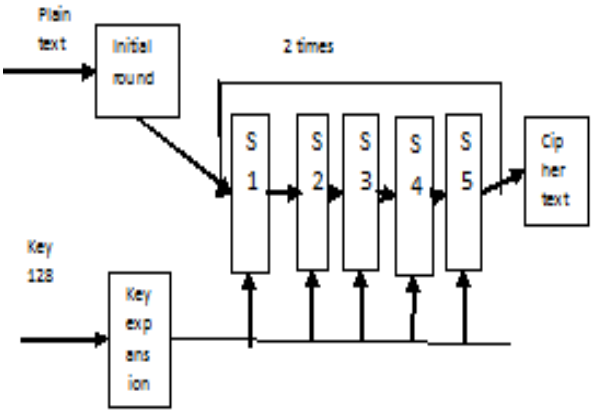

Figure 4.1- Multistage S-Box for IAES

We are presenting a low cost parity based modify (Figure 4.1) scheme for the S-box called Multi stage S-box and the inverse S-box using composite fields. In the presented approach, for increasing the error coverage, the predicted parities of the five blocks of the S-box and the inverse S-box are obtained (three predicted parities for the multiplicative inversion and two for the transformation and affine matrices).

4.1 Algorithm for Proposed multi stage S-box pipeline AES (IAES) -

Algorithm for Multi-stage S-box pipeline AES (IAES)

Input: *Plain text,Byte A[4×nb], Word K[nb ×(nr + 1)];*

Output: *cipher text, Byte C[4×nb]*

4.1.1 IAES Encryption Process-

Bytestate [4, nb]; Set state = A;
AddRoundKey (state, K[0, nb − 1];
for round = 1 to nr − 1
do (repeat step up to end of block)
if(nr mod 2 == 0)
do SubBytes1(state);
ShiftRows(state);
MixColumns(state);
AddRoundKey(state,K[round×nb,nb(round+1))
Else if(nr mod 2 != 0)
do SubBytes2(state);
ShiftRows(state);
Set multi stage s box pipeline for each block
do(Sub_block1+Sub key = Left block 1) *If not left sub block is not up to the mark*
repeat step sub_block1
MixColumns (state);
AddRoundKey(state,K[round×nb,nb(round+1))
End if Stages are not same
Call End loop SubByte
AddRoundKey(state, K[nr × nb, nb(nr + 1) −1]);
C := state;
Repeat step, for all the block

```
return C;
```

4.1.2 IAES Key Expansion Algorithm based on Multistage S-box: Following key expansion algorithm is used in IAES

```
Steps- KeyExpansion(byte key[4*Nk],
word w[Nb*(Nr+1)], Nk
Begin  word temp set i = 0
Check condition while (i < Nk) and
array w[i] = word(key[4*i], key[4*i+1],
  Set key[4*i+2], key[4*i+3])
      Increment i = i+1
end while          and  set i = Nk
repeat  while (i < Nb * (Nr+1)]
copy array values temp = w[i-1]
chek condition if (i mod Nk = 0)
temp = SubWord(RotWord(temp))
                xor Rcon[i/Nk]
   else if (Nk > 6 and i mod Nk = 4)
set  temp = SubWord(temp) end
if    w[i] = w[i-Nk] xor temp
 increment i = i + 1
end while
end
```

4.1.3 IAES Key Decryption Algorithm -Following key expansion algo is used in IAES

```
Steps -InvCipher(byte in[4*Nb],
 byte out[4*Nb], word w[Nb*(Nr+1)])
Begin
      byte state[4,Nb]   and       state = in
Perform AddRoundKey(state,
Call w[Nr*Nb, (Nr+1)*Nb-1])
for round = Nr-1 step -1
do wn to 1
call InvShiftRows(state) and
call InvSubBytes(state)
                use inverse five stage pipline
call AddRoundKey(state,
w[round*Nb, (round+1)*Nb-1])
call InvMixColumns(state)        end
 for     call InvShiftRows(state)  and
                call InvSubBytes(state)
perform AddRoundKey(state,
w[0, Nb-1]),            set out = state
end
```

4.2 Comparison Parameters for AES Vs IAES - Following parameters will be used for result comparison in between AES (Existing) and IAES (Proposed).

1. **Encryption time-**Time that is require to convert a plain text to cipher text.
2. **Decryption time-** Time that is requiring converting a cipher text to plain text.
3. **Encryption speed-** Processor speed/Time that is requires converting a plain text to cipher text.
4. **Decryption speed-** Processor speed/Time Time that is requires converting a cipher text to plain text.

V. CONCLUSION

The AES encryption is widely used and most popular encryption standard. This is also used by different processors. In this research paper presents complete study and performance analysis of existing AES processors. Also suggest performance improvement method of existing, called IAES method .IAES method will be based on new multi stage pipelining s-box and a combinatory logic parallel design with loop unrolling. For performance measurement of AES and proposed IAES different comparison parameters will be calculated for both, in MATLAB environment, such as processor encryption and decryption time and speed for different size of data files.

REFERENCES

[1] Fakir Sharif Hossain1, Md. Liakot Ali, Musadek Anwarul AI Abedin Syed, "A Very Low Power and High Throughput AES Processor, "Proceedings of 14th International Conference on Computer and Information Technology (ICCIT 2011), Dhaka, Bangladesh, 22-24 December,IEEE 2011.

[2] Amish Kumar, Namita Tiwari, "AES Security Enhancement by Using Double S-Box", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3, 3980-3984, ISSN-0975-9646, 2012.

[3] Majithia Sachin,Dinesh Kumar A. Biryukov and I. Nikolic."Automatic search for related-key differential characteristics in byte oriented block ciphers: Application to AES", Camellia, Khazad and others. In H. Gilbert, editor, Advances in Cryptology EUROCRYPT 2010, volume 6110 of Lecture Notes in Computer Science, pages 322–344. Springer Verlag, 2010.

[4] Chih-Pin Su, Chia-Lung Horng, Chih-Tsun Huang_ and Cheng-Wen Wu "A Configurable AES Processor for Enhanced Security" ASP-DAC, IEEE, 2005, pp 99-107.

[5] Kunal Lala, Ajay Kumar ,Amit Kuma, "Enhanced Throughput AES Encryption" International Journal of Electronics and Computer Science Engineering 2132, ISSN- 2277-2012.

[6] O. Prasanthi1, M. Subba Reddy2 "Enhanced AES Algorithm" International Journal of Computer Applications in Engineering Sciences ISSN: 2231 4946, 2012,pp 187-198.

[7] V.S.Jagppati,Binu,S.Subramanian,Piotr,Bilski,Wiesław and Winiecki, 2010 , "Multi core implementation of the symmetric cryptography algorithms in the measurement system",Measurement 43 (2010) 1049–1060,Elsevier.2010 pp321-330

[8] Shaaban sahmoud,wisam elmasry and shadi abudalfa,"ENHANCE MENT the security of AES against modern attack by using variable key block cipher" International Journal of e-technologies, , Vol. 3, No. 1, January 2013.

[9] A. Sekar, S. Radhika ,K. Anand and B.T.Geetha1," Energy Efficient Novel Cipher Security Mechanism For Wireless", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), ISSN 2278-6856 ,Volume 3, Issue 1, January- February 2014

[10] Mark Karpovsky, Konrad J. Kulikowski, and Alexander Taubin Marko Mali "Hardware Implementation of AES Algorithm" Journal of ELECTRICAL ENGINEERING, 2011, Vol. 56, No. 9-10, 2005, 265-269.

[11] Aida Janadi and D. Anas Tarah and Mansoor Ebrahim ,"Symmetric Algorithm Survey: A Comparative Analysis" International Journal of Computer Applications (0975-8887) Volume 61-No.20, January 2013 .

[12] Piotr Bilski , Wiesław Winiecki, "Multi-core implementation of the symmetric cryptography algorithms in the measurement system, Measurement 43"1049–1060, Elsevier. 10.1016/j.measurement.2010.

[13] Hua li and Jianzhou li "A new compact dual-core architecture for AES encryption and decryption Lethbridge,Alberta. Electrical and Computer Engineering, Canadian Journal .10.1109/CJECE.2008.4721627, 2008.

[14] Zhiyong Guo, Guangjun Li, Yang Liu,2010, Dynamic Reconfigurable Implementations of AES Algorithm Based on Pipeline and Parallel Structure,China.ICCET, 10.1109/ICCAE.2010.5451864.

[15] BehrouzA.Forouzan and Debdeep" Cryptography and Network Security" ,The Second International conference on NS,Sydeny 2013.