International Journal for Multidisciplinary Research (IJFMR)
E-ISSN : 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Implementation of AES Algorithm

Aasawari Ujjainkar[1], Prof. A. B. Kharate[2]

[1]Student, Department of Electronics & Telecommunication Engineering, Amaravati University, Amravati
[2]Professor, Department of Electronics & Telecommunication Engineering, Amaravati University, Amravati

***Abstract*: Now a day's large number of internet and wireless communication users has led to an increasing demand of security measures and devices for protecting the user data transmitted over the unsecured network so that unauthorized persons cannot access it. As we share the data through wireless network it should provide data confidentiality, integrity and authentication. The symmetric block cipher plays a major role in the bulk data encryption. Advanced Encryption Standard (AES) provides data security. AES has the advantage of being implemented in both hardware and software. Hardware implementation of the AES has lot of advantage such has increased throughput and better security level. Hardware Implementation for 128-bit AES (Advanced Encryption Standard) encryption and Decryption has been made using VHDL. The proposed algorithm for encryption and decryption module will functionally verified using modelsim, will be synthesize using Quartus 2 using Altera FPGA platform and analyze the design for the power, Throughput & area.**

***Keywords*: AES, Encryption, Decryption, FPGA, VHDL, Security**

INTRODUCTION

Advance encryption standard find its rout in cryptography and network security, Because of cryptography, doing business electronically is possible without worries of deceit and deception. Cryptography technology has changed the world today by being able to carry data found in the physical world to the electronic world with confidence. Nowadays, hundreds of thousands of people interact electronically every day, whether it is through email, E-commerce, E-bank or cellular phones. As the network transmission speed upgrades to the gigabits per second (Gbps), the software-based implementations of cryptographic algorithms cannot meet its needs. The hardware-based implementations can greatly improve throughput and reduce the key generation time. Besides, the processes of cryptographic algorithms and the key generation packaged in chip, which cannot easily be read or changed by external attacker, so hardware-based implementations can get the higher physical security. In recent years, many hardware based Implementations use the field programmable gate arrays (FPGA) and the application specific integrated circuit (ASIC) ASIC lacks of flexibility and has high development costs and long development cycle. Reconfigurable devices such as FPGA, with hardware of security and high speed and software of flexibility and easy maintenance, have become hardware-based implementations research hotspots for block cipher algorithm.

1. BACKGROUND

As we know, the security strength of Data Encryption Standard (DES) [1] has been difficult to adapt to new needs. In October of 2000, the National Institute of Standards and Technology (NIST) selected the

Rijndael algorithm as the advanced encryption standard (AES), which was developed by Joan Daemen and Vincent Rijmen, in order to replace the DES. At present, Rijndael is the most common and widely used symmetric cryptosystem to support bulk data encryption. It offers a good "combination of flexibility, efficiency and safety". AES is the abbreviation of Advanced Encryption Standard also known as Rijndael algorithm. It is symmetrical block cipher which uses the same key for both encryption and decryption. The minimum length specified can be 128, 192 and 256 bits.

2. ALGORITHM DESCRIPTION

2.1 Byte Substation

Each byte of the state is substituted with a 8-bit value from the S-box. The S-box contains a permutation of all possible 256 8-bit values. It is a nonlinear operation and the only non-linear transformation in this procedure. The S-box is gained by a multiplicative inverse over GF(2^8) and an affine transform.The sub bytes operation is required for both encryption and key expansion and its inverse is done for decryption. Its implementation has a direct impact on the overall throughput.

2.2 Shift Row Operation

Shift Rows it is relatively simple. State is the intermediate cipher result that can be pictured as a rectangular array of bytes, having four rows. In the direct ShiftRows transformation, the first line of State remains the same, the second line, third line and fourth line respectively ring shift left 1byte, 2 bytes, and 3bytes.

2.3 Mixcolumn

MixColumn operation performs on the state column by column, treating each column as a four-term polynomial over GF (2^8).As a result of this multiplication, the new four bytes in a column is generated as follow:

$$A = (\{02\} \cdot A) \otimes (\{03\} \cdot B) \otimes (\{01\} \cdot C) \otimes (\{01\} \cdot D)$$

$$B = (\{01\} \cdot A) \otimes (\{02\} \cdot B) \otimes (\{03\} \cdot C) \otimes (\{01\} \cdot D)$$

$$C = (\{01\} \cdot A) \otimes (\{01\} \cdot B) \otimes (\{02\} \cdot C) \otimes (\{03\} \cdot D)$$

$$C = (\{03\} \cdot A) \otimes (\{01\} \cdot B) \otimes (\{01\} \cdot C) \otimes (\{02\} \cdot D)$$

The operation of „ " is XOR operation modulo 2 and the „ " is a multiplication of polynomials modulo an irreducible polynomial $m(x) = x^8+x^4+x^3+x+1$.

2.4 Add round key

The transformation in the cipher and inverse cipher in which a round key is added to the state using an XOR operation. Round keys are values derived from the cipher key using the Key Expansion routine.

2.5 Key expansion

It is the routine used to generate a series of Round Keys from the cipher key KeyExpansion is carried out for the word, and to this two word processing functions are introduced which are word substitution (Subword) and word rotation (RotWord). Subword takes a four-byte input word and applies an S-box to each of the four bytes to produce an output word. RotWord takes a four-byte word and performs a cyclic permutation.

3 PROPOSED SYSTEM

AES cipher is operating on data blocks having the length of 128 bits with a symmetric key, which may have a length of 128, 196 or 256 bits. Operations are performed on a matrix of size 4 x 4 bytes called the state. The algorithm consists of successive steps. First, the data stored in the state array are added mod 2 with the master key by the operation AddRoundKey. The next steps are rounds repeated Nr times.Each round performs 4 successive operations: (1) substitution of bytes SubBytes, (2) rows shifting ShiftRows, (3) mixing of columns MixColumn, and (4) AddRoundKey. The number of rounds Nr depends on the key length; for the 128-bit key Nr = 10. The last step performs 3 operations: Sub- Bytes, ShiftRows and AddRoundKey. At each step another key generated as an extension by the procedure KeyExpansionis added.

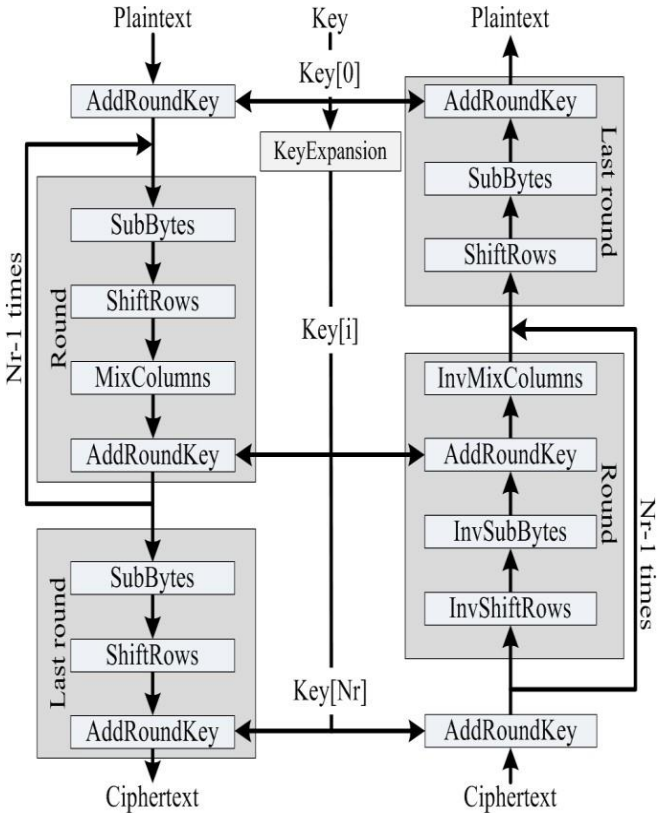


Figure 1 Block diagram of proposed system

Whereas the decryption process are relatively executing the same process as what encryption is doing except it is performing the inverse of the encryption process which are Inverse Subbytes, Inverse Shiftrow, Inverse mixcolumn and Inverse AddRoundkey[2]. This paper will describes both encryption and decryption process the block diagram of proposed system is shown in figure 1.

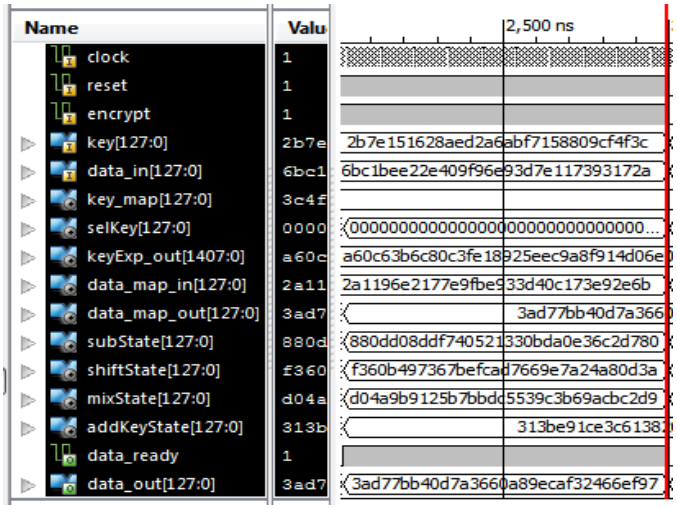
4 RESULTS

The verification was done using the test vector and the expected output as described in the fips-197, Appendix B section [1]. The architecture of this AES works as expected foreach process as described in Figure A. The cipher is progressed using the round key value and the input shown in Table 1, when the ready signal is high the data is fully encrypted, i.e. the output/data_out as shown in Figure 2.the decryption data data_out is shown in Fig 3.

Table -1: Example test vector

Key	2b7e151628aed2a6abf7158809cf4f3c
Plain text	6bc1bee22e409f96e93d7e117393172a
Cipher text	3ad77bb40d7a3660a89ecaf32466ef97

Figure 2 Encryption simulation waveforms



RTL diagram of proposed system

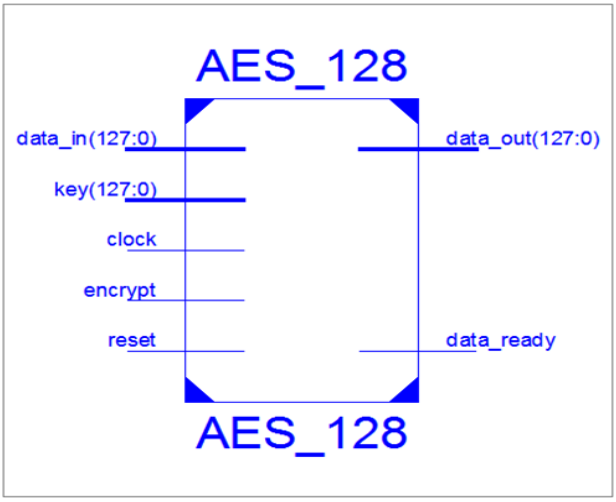


Figure 3 RTL diagram

5 CONCLUSIONS

In this paper Advanced Encryption Standard (AES) algorithm is implemented, that can process with the data block of 128 bit and cipher key length of 128 bit. The usage of 128 bit cipher key to achieve the high security, because 128 bit cipher key is difficult to broken. As result of this we obtain a secure transmission of data in both encryption and decryption. While computing the existing AES, it takes more area.

REFERENCES

1. NIST, Advanced Encryption Standard (AES), (FIP PUB 197) http://csrc.nist.gov/publications
2. Rozita Borhan, Raja Mohd Fuad Tengku Aziz,"Successful Implementation of AES Algorithm in Hardware" 2012 IEEE International conference on Electronics Design, system and application(ICEDSA)
3. William Stallings "Cryptography and network Security" Principles and practise Fourth Edition
4. Morris Dworkin, "Recommendation for n BlockCipher Modes of Operation" Methods and Techniques. NIST Special Publication 800-38A 2001 Edition
5. S, Lara, Accelerating algorithms in hardware, datevisited:(10/06/2008) http://www.embedded.com/show/ Article.jhtml?articleID=175 00157
6. N Dave, AES Encryption is Cracked, 2011, date visited (22/11/2012) http://www.theinquirer.net/inquirer/news/2102435/aesencryption cracked