ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, Vol 9(47), DOI: 10.17485/ijst/2016/v9i47/106810, December 2016 ISSN (Online) : 0974-5645

Implementation and Analysis of Triple AES in VHDL

Gagandeep Singh Walia*, Narinder Pal Singh, Hunny Pahuja and Amandeep Singh

Department of Electronics and Communication Engineering, India;
gagandeep.19715@lpu.co.in, er.narinderpal@gmail.com, hunny.20429@lpu.co.in, singh_aman099@yahoo.com

Abstract

Successful secure data communication requires encryption of the data by a certain algorithm to keep it safe from unauthorized access. One such algorithm is Triple. Advance Encrypting Standard which differs from AES by using three keys for encryption. It uses same Rijndael's AES Algorithm but has more reliability and longer key length. AES uses symmetric keys due to which data can be accessed by unauthorized users if they get the key. So the proposed system works on using three different keys to encrypt the data so that all these keys are required to successfully decrypt the data. The cryptographic algorithm is modified in such a way that the final result cannot be cracked even if intermediate data appears as such. This paper also provides comparative analysis of DES i.e. Data Encrypting Standard, Triple DES, AES and Triple AES.

Keywords: AES, Cryptography, Decryption, Encryption, Triple AES

1. Introduction

In any communication system, wireless devices and many other applications, the data security is considered an important factor. Numerous technologies and algorithms have been built to secure data and protect it from assorted hackers and unauthorized admittance. With changing technology, hackers, electronic eavesdropping etc. have developed new techniques to attack the data. Cryptography is a technique to encrypt and decrypt data by the use of mathematics. It enables the storage of information that is sensitive or it transmits over the networks which are not secured so that nobody other than the intended recipient should be able to read it.

Several encrypting algorithm have been built to deal with data security attacks. One such algorithm is Advanced Encrypting Standard (AES) which is issued by FIPS by National Institute of Standards and Technology (NIST)[1].

For conventional encryption, basic requirements needed are:

Requirement of a strong encryption algorithm so that an individual who has knowledge of the algorithm and may be able to access more than one cipher texts shall not be able to read or decipher cipher text or to find out the way to have the key. The copy of the secret key must be present with both the transmitter and the recipient in a secure way.

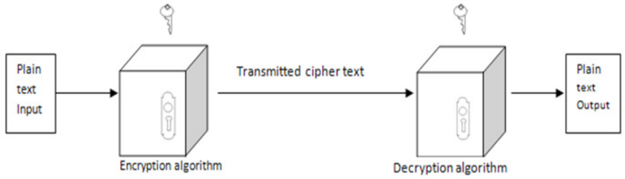


Figure 1. Model of conventional cryptosystem.

Figure 1 shows the model for conventional cryptosystem. Two cryptographers who belongs to Belgium developed the cipher based Advanced Encryption Standard. Rijndael is a family of ciphers having various block and key and these all are different from each other. The size of the block is 128 bits and the various lengths of the key are of 128, 192 and 256 bits. AES operates on a 4×4 column-major order matrix of bytes termed the state. For the conversion of plaintext into the cipher text, it requires many repetitions of transformation rounds and this is specified by size of key used in AES cipher:

*Author for correspondence

For 128 bit keys 10 cycles of repetition are required.
For 192 bit keys 12 cycles of repetition are required.
For 256 bit keys 14 cycles of repetition are required.

Each round consists of a series of processing steps. Every round consists of four different stages but similar pertaining to the fact that one that depends on the encryption key itself. The cipher text is transformed back to the original plaintext with the usage of same encryption key and this transformation is achieved with the help of set of reverse rounds[2].

2. Proposed System

Triple AES is a process to reuse implementations of AES with serial installation of three instances of AES to improve the security of the data. In the process of encryption, use of three keys leads to the formation of triple AES. The AES operation is performed three times with three different keys. K1, K2 and K3 are the three different keys used on a plain text P to convert it into cipher text C. By using the Rijndael algorithm, the encryption E1 is done with the help of key K1 and the result of this is fed to encryption E2 having key K2 and third encryption E3 is performed with key K3. Multi encryption of the data increases its security and makes it difficult to decode or crack the data. Figure 2 shows the model for implementing triple AES.

The decrypting procedure is same as encryption procedure but executed in reverse[6]. Some keys can make the encryption weak i.e. if second or first key or the third or second key is same. This encryption procedure will almost be same as the encryption procedure for standard AES.

The Triple AES encryption is done as:

Encryption along with K1
Encryption along with K2
Encryption along with K3

The Decryption is the reverse process of the encryption and done as:

Decryption along with K3
Decryption along with K2
Decryption along with K1

3. Rijndael Algo

An Algorithm was suggested by Rijndael that connects a data block which is variable and length of key is also variable. It is an iterative block cipher which is of 128 bits, 192 bits or 256 bits and he gave the name to this algorithm as AES algorithm. The basic working of AES is to perform identical steps several times. The basic criteria of design incorporated for AES algorithm is that its implementation can be done both in software and hardware while DES can only be implemented in hardware[7].

On implementation, every cycle of algorithm in the network retrieves a new round key from the key scheduling algorithm. The state in the AES proposal is the intermediate result of the cipher which is retrieved at the completion of each cycle. A key scheduling algorithm has been designed which states that in every cycle, Modulo 2 operation of the plaintext and the key is carried out in order to expand the original key into several Round Keys. Many sub keys are derived from the main key for the functioning of each cycle and the method of deriving sub keys from the parent key is referred to as key expansion unit[8].

4. Comparison

User needs and task accomplishment determines the choice between DES, 3DES, AES and 3AES. DES was mainly required to perform well in hardware as compared to software. DES performs lots of bit manipulation in substitution and permutation. For better security and safety,

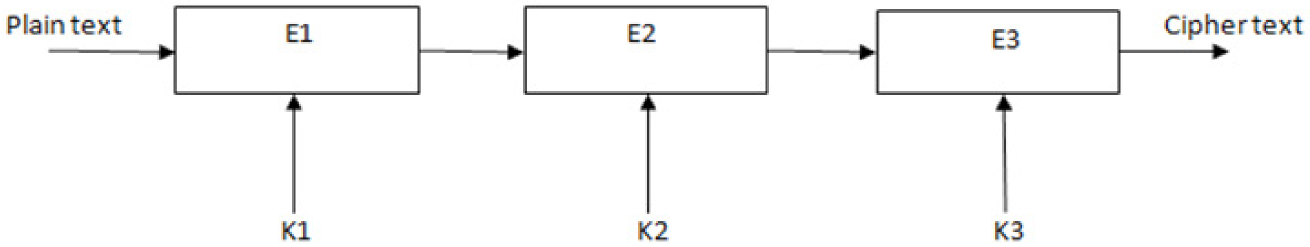


Figure 2. Model of triple AES.

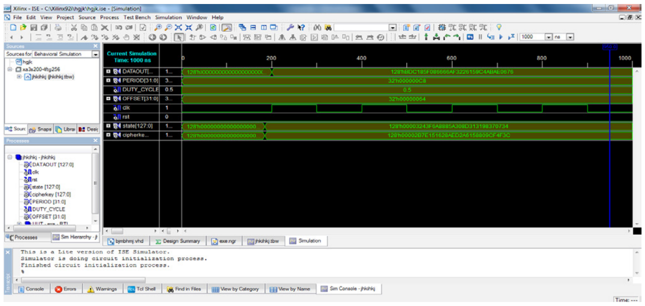
Table 1. Comparison DES, 3DES, AES & 3AES

Distinguishing Parameters	DES	3DES	AES	3AES
Key Size	56 bits	112 or 168 bits (depending on keys used)	128,192 or 256 bits	128,192 or 256 bits
Algorithm's Time	Symmetric	Symmetric	Symmetric	Symmetric
Speed	Low	Moderate	High	High
Consumption Of Resource	High	Moderate	Low	Moderate
Security	Proven inadequate	Still insecure	Secure	More Secure
Block Size	64bits	64bits	128,192 or 256bits	128 bits,192 bits or 256bits
Crack Time	64bit key- 400 days	112bit key- 800 days	128bit key- 5×10^{21}years	128 bit key - 3.31×10^{56} years
Possible Ascii Printable Character	95^{7}	95^{14}or95^{21}	95^{16} or 95^{24} or95^{32}	95^{48}
Rounds	16	48	10(128bits), 12(192bits) , 14(256bits)	10(128bits), 12(192bits), 14(256bits)
Key	Single	Single (later divided in 3parts)	Single	Three

power testing resistance, hardware and software recital, Advance Encryption Standard (AES) was developed[3,4]. Table 1 represents the comparative analysis of different encryption standards with triple AES.

5. Result

Xilinx-9.2i is used for synthesizing the proposed system and the simulation is done in Xilinx ISE Simulator. The simulation result for 128 bit key using triple AES is computed by Xilinx ISE 9.1i. Figure 3 shows the test bench waveform of the proposed algorithm.


Xilinx - ISE - C:\Xilinx92i\hgjk\hgjk.ise - [Simulation]
File Edit View Project Source Process Test Bench Simulation Window Help
Current Simulation Time: 1000 ns
0 200 400 600 800 1000
DATAOUT[... 128'hXXXXXXXXXXXXXXXXXXX 128'hBDC185F086666AF3226159C4ABAE0676
PERIOD[31:0] 32'h000000C8
DUTY_CYCLE 0.5
OFFSET[31:0] 32'h00000064
clk 1
rst 0
state[127:0] 128'h00003243F6A8885A308D313198370734
cipherke... 128'h00002B7E151628AED2A6158809CF4F3C
Sources for: Behavioral Simulation
hgjk
xa3s200-4ftg256
jhkihkj (jhkihkj.tbw)
jhkihkj - jhkihkj
DATAOUT [127:0]
clk
rst
state [127:0]
cipherkey [127:0]
PERIOD [31:0]
DUTY_CYCLE
OFFSET [31:0]
Processes
Sim Hierarchy
bjmbhmj.vhd
Design Summary
exe.ngr
jhkihkj.tbw
Simulation
Console
Errors
Warnings
Tcl Shell
Find in Files
View by Category
View by Name
Sim Console - jhkihkj

```
This is a Lite version of ISE Simulator.
Simulator is doing circuit initialization process.
Finished circuit initialization process.
```

Figure 3. Simulation waveform.

Figure 4 defines the RTL schematic for such algorithm defining the hardware implementation. It shows different blocks, their inputs and outputs used to implement such a system in a practical environment.

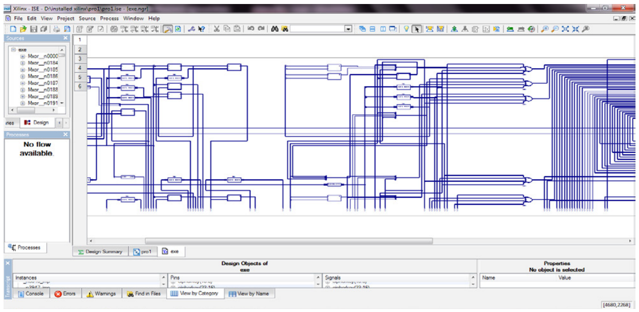


Figure 4. RTL Schematic.

6. Conclusion

Due to the needs in communications for more safe and secure, a new variation of AES has been proposed and implemented. In this paper, the AES using three keys has been designed and results are verified. The performance comparison of Triple AES with different encryption standards are obtained in term of security, time to crack and resources utilization. The throughput is increased because of the greater input block and the security of the algorithm is achieved due to greater key size. The area required is more but it can be neglected. This algorithm is best for applications in which very high security and increased throughput is required such as in multimedia communications.

7. References

1. Su CP, Lin TF, Huang CT, Wu CW. A high throughput low cost AES processor. IEEE Communications Magazine. 2003; 41(13).
2. Khatri N, Dhanda R, Singh J. Comparison of power consumption and strict avalanche criteria at encryption/decryption side of different AES standards. International Journal of Computational Engineering Research. 2012; 2(4).
3. Hamdan O, Alanazi, Zaidan BB, Zaidan AA, Jalab HA, Shabbir M, Al-Nabhani Y. New Comparative Study between DES. 3DES and AES.
4. Mohan HS, Raji Reddy A. Performance analysis of AES and MARS encryption algorithm. International Journal of Computer Science Issues. 2011; 8(4)
5. Kumar A, Tiwari N. Efficient implementation and avalanche effect of AES. IJSPTM. 2012; 1(3/4).
6. Zhang X, Parhi KK. Implementation approaches for the advanced encryption standard algorithm. IEEE Transactions. 2002.
7. Daemen J, Rijmen V. AES Proposal: Rijndael. AES Algorithm Submission. 2005 Sep 3.
8. Daemen J, Rijmen V. The Block Cipher Rijndael, Smart Card Research and Applications, LNCS 1820. Springer-Verlag; p. 288-96.