ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Image Encryption & Decryption by AES 128 BIT Core using FPGA Implementation

S. Sai Sabarish
M.Tech Student,
Department of ECE,
St. Peter's Engineering College,
Hyderabad, Telangana.

N. Ratna Deepthika
Assistant Professor,
Department of ECE,
St. Peter's Engineering College,
Hyderabad, Telangana.

INTRODUCTION

Cryptography is a technique, rapidly used to protect the information in recent innovations. Cryptography is the science of secret codes, which enables the confidentiality of communication through an insecure channel. This protects against unauthorized parties by preventing unauthorized alteration of use. It uses a cryptographic technique that transform a plaintext into a cipher text using most of the time a key, where AES Algorithm, DES algorithm, Triple DES are some examples. There exists certain cipher that doesn't need a key at all. An example for this type is a simple Caesar-cipher that obscures text by replacing each letter with the letter thirteen places down in the alphabet. Since our alphabet has 26 characters, it is enough to encrypt the cipher text again to retrieve the original message.

TERMS USED IN CRYPTOGRAPHY

Plain Text

Plain text or clear text is the original data that the user can read and understand. In cryptography the original information need to send other individual is called as plain text is before being encrypted into cipher text or after being decrypted. Suppose a person wishes to send "hello world" message to other person. Here "hello world" is a plain text message.

Cipher Text

Cipher text or Hypertext is a meaningless message that can readable but cannot be understood by anyone. Before the transmission of actual message it is transformed into meaningless unreadable message by using a crypto system.

For example "1A#$GT^$&$$5%" is a cipher text produced for "hello world".

Encryption

Encryption is down at the sender side. It is a process of translating a message, called the Plaintext, into an encoded message, called the Cipher text. Using cryptography we can send the message confidentially through an unreliable channel. The encryption process encapsulates two things a secret key and an encryption algorithm.

Decryption

Decryption takes place at receiver side to get the original message from unreadable data. Decryption is a reverse process of encryption that is translating a cipher text into plain text. The decryption process also having two things a secret key and a decrypting algorithm. Generally the encryption and decryption algorithms are same and the secret key also same for encryption and decryption.

Key

The key is used when encrypting the plain text at the sender side and when the decryption takes place on the cipher text at receiver side. Generally a key may be a numeric or alpha numeric or special character. The secret key is main requirement of symmetric key algorithms. The stream generation in cryptography is very important because the maximum security of an algorithm is depends on secret key. The secret transmission of secret key is more important as if intruders know the secret key they can analyze the plain text from cipher text easily

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

CONVENTIONAL ENCRYPTION

Conventional encryption is the process that reduces the difficulty of sending a huge data in secret into sending a small data in secret that is called cipher key.

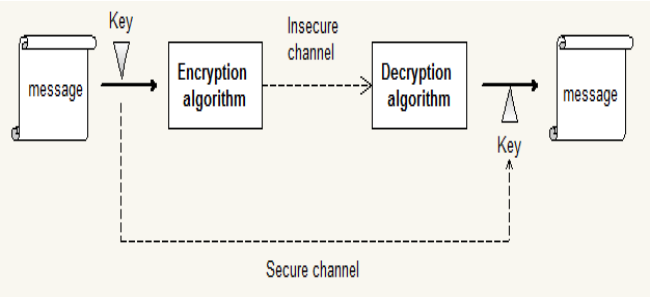


Fig 1. Conventional encryption

Basic Encryption

A message being encrypted is referred to as the plaintext. The plaintext is fed into an encryption algorithm, which has a special parameter known as a key. The output of this algorithm, called the ciphertext, is transmitted to the receiver over an insecure channel, The receiver can recover the plaintext by running a decryption algorithm, which also has a key as a parameter.The key is send to the receiver via secure channel. Figure 1 gives the basic layout of an encryption algorithm.

Algorithm is the mathematical function used for encryption and decryption. If the security of an algorithm is based on its secrecy than it is called as restricted algorithm. A large associate organizers are not able to utilize them, due to an organizer can leaves the association frequently, all organizers algorithm must be change. Of course the restricted algorithms can allowed to use without quality control or standardizations. But these are enormously popular for low security applications. We can solve this problem by using modern cryptography with a key (k). Both encrypting and decrypting operations uses same key. So the encryption and decryption functions become;

E_k (M) = C for encryption E_k→ Encryption using key k, M→message

D_k (C) = M for decryption D_k→ Decryption using key k, C→cipher text

PROPOSED WORK

The objective of this project is to encrypt and decrypt of an image data. An image data cannot pass directly to the AES, So, there is necessary to implement any one of communication interface to transferring an image to AES Core. In this implementation UART is opted as communication interface for AES 128-bit core. It has several hardware blocks such as UART, AES encryption and decryption block.

AES ENCRYPTION

AES is supported for both encryption and decryption for any kind of data. There are several standard type of bit lengths and along with symmetric Keys are used in AES such as 128,192,256-bits.Here, in this paper 128-bit standard AES core is used. AES has several steps such as adding plain text, adding symmetric Key, shifting rows and columns, mixed columns, substitution box contains subbytes and shift rows. All these blocks are used for encryption process. A brief overview of AES Encryption process as shown in figure3.1

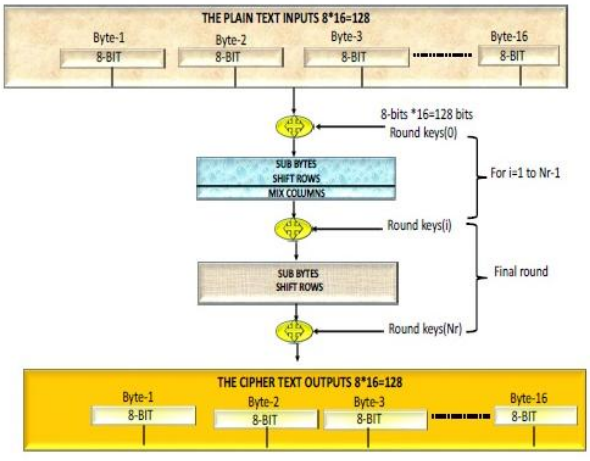


Fig 2. Encryption Process

Initially, two inputs are given to the AES such as 128-bit data and 128-bit symmetric key (cipher key). At first 128-bit data is divided in to 16 bytes, and each byte consist of 8-bit length.The basic step is to make an XOR operation between plain text and add round key and then next operation will be performed. First

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

step is non-linear substitution box transformation in that each byte is inverted independently and it can be performed by using look-up table. The total substitution box contains 4x4 matrix and all these substitution transformation is done in one clock cycle and it can be called as S-box transformation.

Second step shift row operation is performed in that first row is unchanged, second row rotate shift left by one byte, third row rotate shift left by two bytes, fourth row rotate shift left by three bytes. This process can be called as shift row transformation.

Third step is Mix-columns transformation is performed. In this mix-column transformation contains 4x4 matrix in that, states are considered as polynomial over Galois Field GF(28) and multiplied modulo X4 + 1 with fixed polynomial. This process is known as Mix-column transformation.

Fourth step is add round key, in this step, add round key is added to the output of Mix column transformation by making simple XOR operation. Each round has one distinctive key which is generated from maim key. So, totally 10 rounds are taken place with 11 distinctive keys which is generated from cipher key. Then this total number of 10 rounds are essential to encrypt the data.

Similarly, the same steps are inversely happen in decryption process. The decryption steps are like inv-sub bytes, invshift rows, inv-Mixcolumns, add round key.

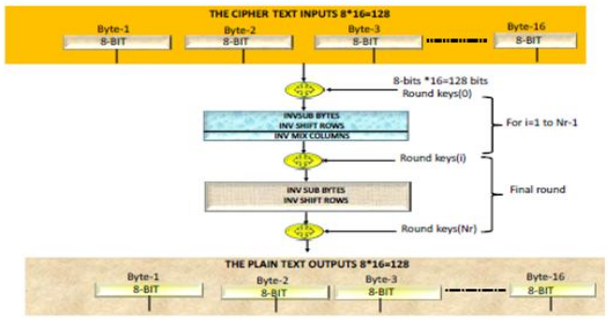


Fig 3. Decryption Process

FPGA IMPLEMENTATION PROCESS OF AES-128 BIT CORE INTERFACE WITH UART:

FPGA implementation of image encryption and decryption process has many blocks such as UART receiver & transmitter, Buffer/RAM, clock generator, counter, FSM control, 16x1 Mux, AES-128 bit core. Here, an image is considered as an input with the size of 4096 bytes.

An image is converted into hexadecimal values and each byte is transferred through UART. UART receiver can receive only 8-bits at a time. So, that the inputs are driven into the dual port memory which can be used for storing and retrieving purpose. The dual port memory size is 128 bit and each 128 bit is considered as one block of data. So, the target size is 4096 bytes then totally 256 blocks of data needed to receive. The number of blocks of data is measured by the counter. After receiving each block of data it should be transferred to the AES 128-bit core. Here, the UART, Dual port memory, counter and AES-128 bit core are controlled by the finite state machine design. AES input key is fixed and another data input is getting from dual port buffer. The output size of AES is 128 bit and each 128-bit is divided in to 16 bytes. Each output byte is transferred to UART transmitter by 16x1 MUX.

Here, the UART baudrate at the receiver and transmitter is set to 9600 bits per second. So, there is some essential calculations are required to transfer each bit.
According to the given baud rate is 9600,
Given baudrate = 9600bits=second So,
Each bit = 1=9600sec = 104usec:
Assume applied FPGA clock frequency is 50 Mhz and this clock frequency is converted into 20ns. Therefore, to transfer each bit is equal to given baud rate multiplied by applied clock frequency.
Each bit = 104usec _ 50 Mhz = 104000ns=20ns =5200cyles
In this regard we cannot monitor those many clock cycles, so to increase the sample rate by 16 i.e, 1 bit =

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

5200/16 = 325cycles So, by this we can determine the glitch problems by monitoring for every 8 clock cycles.

Therefore, FPGA implementation of AES decryption is as followed the same step implemented in AES encryption. Here, only difference is encrypted image is taken as an input and at the final output is decrypted image.

SIMULATION RESULTS WITH PERFORMANCE ANALYSIS

AES encryption and decryption simulation is done by using Xilinx ISIM. Simulation and test bench process. The input image is converted in to Hexadecimal code using matlab. The size of the image is 4096 bytes converted in to 64x64 bytes. This hexadecimal data considered as an input for AES. Initially, the input data is read by memory after storing into the memory then byte by byte has to be transferred for UART transmitter.

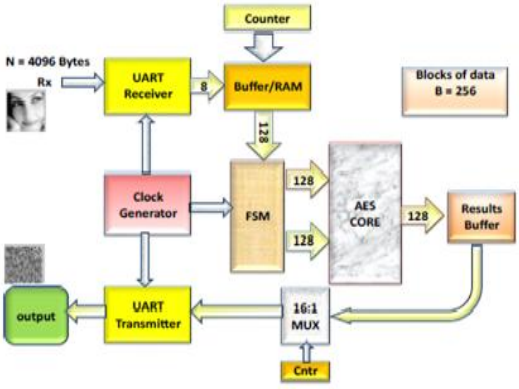


Fig 4. FPGA Implementation Process Of AES-128 Bit Core Interface With UART

For each byte of data delayed with 100ns. At the receiver side, UART receiver is receiving byte by byte and it is stored in file called crypto image.txt. The total amount of time taken for image encryption process is about 5358995ns. In the same way, decryption process is also done, but the only difference is crypto image.txt considered as an input and at the final output is decipher image.txt.

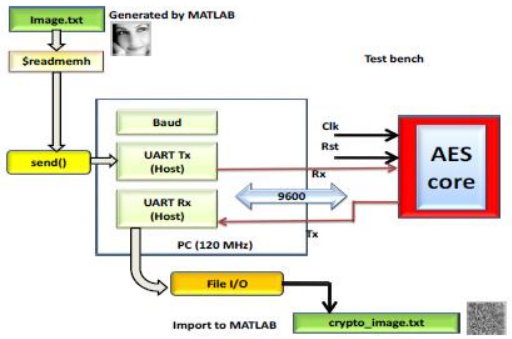


Fig 5. Simulation And Test bench Process Of AES

A. PERFORMANCE ANALYSIS:

The performance analysis of AES encryption and decryption is described here. According to the synthesis report, the amount of latency is taken for 128-bits to encrypt about 8.705 ns and similarly, for decryption is about 7.770ns. Therefore, the latency difference between encryption and decryption is 0.935 ns. Due to this difference there is some noise presented in the decrypted image. In the decryption process there is some packets are missing this is because of UART communication. The total amount of area occupied for encryption is 6%of slices, 2% of slice Flip flops, 5% of 4-input LUTS and44% of BRAMS, and the total amount of power consumption is 441.91 mW for encryption. Similarly, the amount of area occupied for decryption is 7% of slices, 2% of slice Flipflops, 7% of 4-input LUTS and 55% of BRAMS, and the total amount of power consumption is 442 mW. The amount of area and power consumption is exceed about1% in decryption.

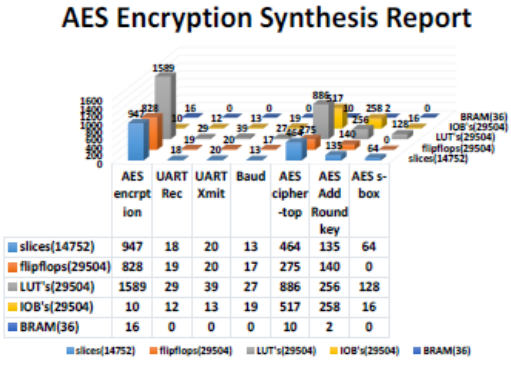
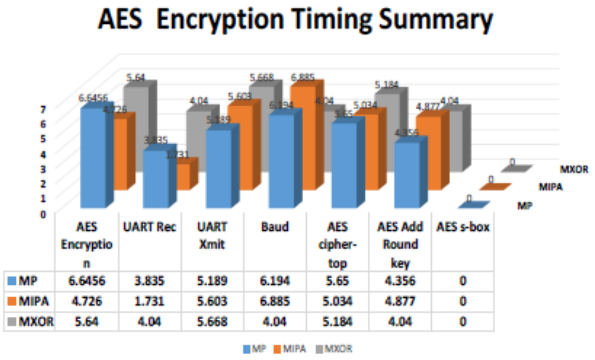


Fig 6. Synthesis Report Of AES Encryption

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

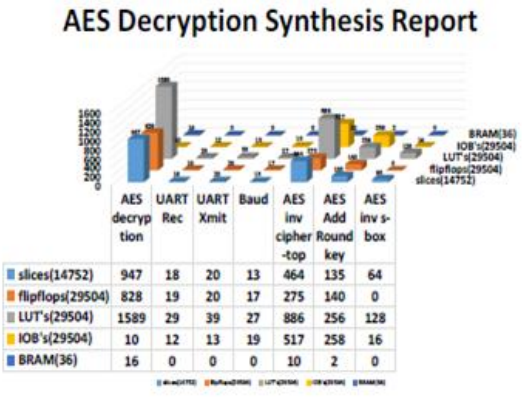
In this synthesis report, total amount of area occupied for encryption is 6% of slices, 2% of slice Flip flops, 5% of 4- input LUTs and 44% of BRAMs. A detailed report with graph representation as shown in fig 6.



	AES Encryption	UART Rec	UART Xmit	Baud	AES cipher-top	AES Add Round key	AES s-box
MP	6.6456	3.835	5.189	6.194	5.65	4.356	0
MIPA	4.726	1.731	5.603	6.885	5.034	4.877	0
MXOR	5.64	4.04	5.668	4.04	5.184	4.04	0

Fig 7. Timing Report Of AES Encryption
MP:Minimum Time Period(ns)
MIPA:Minimum Input Arrival Time(ns)
MXOR:Maximum Output Required Time(ns)

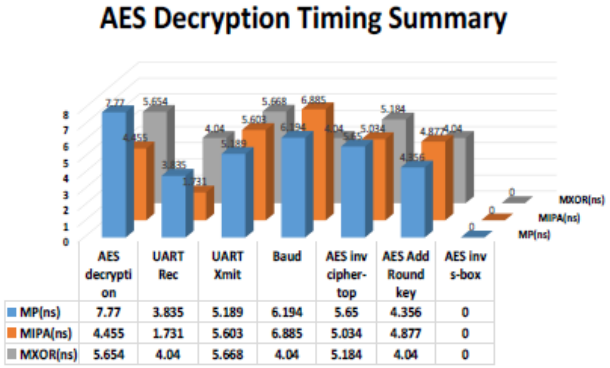
In fig7. overall timing summary for encryption is 6.6456ns, minimum input arrival time 4.726ns and maximum output required time 5.64ns.Here the encryption add round key alone minimum amount of time period is 4.356ns and along with some of the individual timing summary as represented in terms of table with graph.



	AES decryption	UART Rec	UART Xmit	Baud	AES inv cipher-top	AES Add Round key	AES inv s-box
slices(14752)	947	18	20	13	464	135	64
flipflops(29504)	828	19	20	17	275	140	0
LUT's(29504)	1589	29	39	27	886	256	128
IOB's(29504)	10	12	13	19	517	258	16
BRAM(36)	16	0	0	0	10	2	0

Fig 8. Synthesis Report of AES Decryption

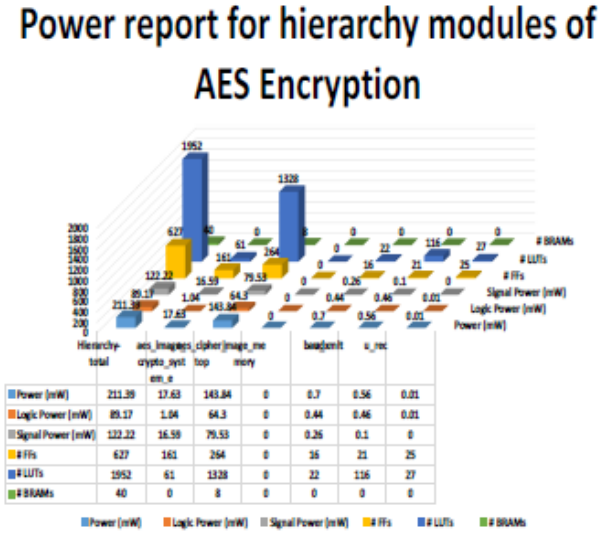
In this synthesis report, total amount of area occupied for decryption is 7% of slices, 2% of slice Flip flops, 7% of 4- input LUTs and 55% of BRAMs. A detailed report with graph representation as shown in fig 8.



	AES decryption	UART Rec	UART Xmit	Baud	AES inv cipher-top	AES Add Round key	AES inv s-box
MP(ns)	7.77	3.835	5.189	6.194	5.65	4.356	0
MIPA(ns)	4.455	1.731	5.603	6.885	5.034	4.877	0
MXOR(ns)	5.654	4.04	5.668	4.04	5.184	4.04	0

Fig 9. Timing Report Of AES Decryption
MP:Minimum Time Period(ns)
MIPA:Minimum Input Arrival Time(ns)
MXOR:Maximum Output Required Time(ns)

In fig 9. overall timing summary for encryption is 7.77ns, minimum input arrival time 4.455ns and maximum output required time is 5.654ns. Here the decryption add round key alone minimum amount of time period is 4.356ns and along with some of the individual timing summary as represented in terms of table with graph.



	Hierarchy-total	aes_images_crypto_system	cipher_top	image_memory	baud_xmit	s_rec
Power (mW)	211.39	17.63	143.84	0	0.7	0.56	0.01
Logic Power (mW)	89.17	1.04	64.3	0	0.44	0.46	0.01
Signal Power (mW)	122.22	16.59	79.53	0	0.26	0.1	0
# FFs	627	161	264	0	16	21	25
# LUTs	1952	61	1328	0	22	116	27
# BRAMs	40	0	8	0	0	0	0

Fig 10. Power Report Of AES Encryption

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

In fig 10. overall static power summary report for encryption is 211.39mW and along with some of the individual modules of power report as represented in terms of table with graph.

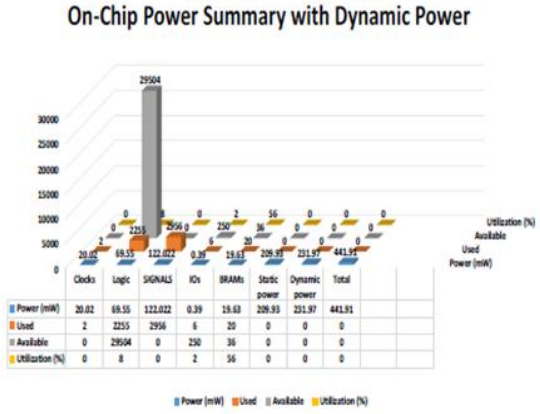


Fig 11. On Chip Power Summary Report Of AES Encryption

In fig 11. overall on-chip power summary report with dynamic power for encryption is 441.91mW and along with some of the individual modules of power report as represented in terms of table with graph.

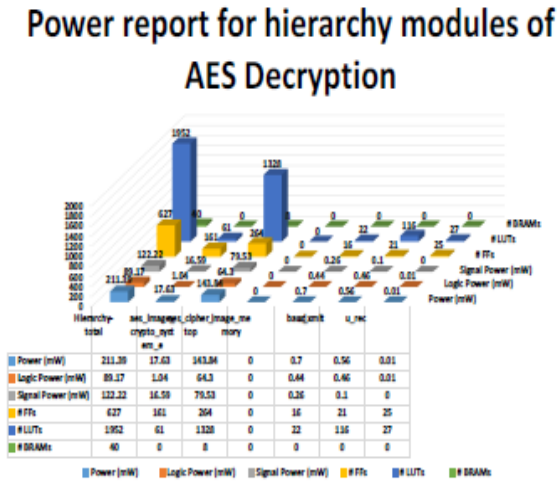


Fig 12. Power Report Of AES Decryption

In fig 12, overall static power summary report for encryption is 211.39mW and along with some of the individual modules of power report as represented in terms of table with graph.

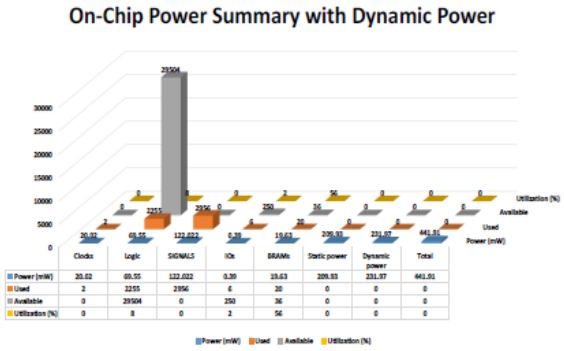


Fig 13. On Chip Power Summary Report Of AES Decryption

In fig 13, overall on-chip power summary report with dynamic power for encryption is 442mW and along with some of the individual modules of power report as represented in terms of table with graph.

ADVANTAGES AND APPLICATIONS

ADVANTAGES

- FPGA implementation gives better speeds compared to software implementation
- AES is Private Key Symmetric block Cipher. So more secure.
- Stronger & faster than Triple-DES

APPLICATIONS

- In hardware accelerator cards for e-commerce servers and secure trunk communications.
- In PDA, Wireless network and embedded devices.

Commercial Applications:

Encryption is necessary to secure electronic communication. However, the process of encryption and decryption is overhead, that is, it is computation intensive, does not involve retrieval, movement or storage of data and is common to every transaction. For example, if the encryption and decryption processes were to be handled by a hardware interface (such as one based on the product described in this project), the infrastructure required to operate a secure web service would be minimised.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A similar argument would apply to the use of this product in communications, the military, IT, and electronic payment systems: there can be a cost-efficient improvement in performance if a task common to every transaction is delegated to appropriate hardware.

CONCLUSION

In this project, image encryption and decryption algorithm implemented by using AES 128-bit core. Here, the experimental results are measured and compared with respect to area, power, and latency. The amount of area and power consumption is exceeded about 1% in decryption. Here, not only that there is some noise presented in decryption because of the latency variation. This problem is because of UART communication. Due to this latency variation between encryption and decryption, UART communication is not well supported. Therefore, instead of using UART, Ethernet is more speed and it can avoid the loss of packets.

REFERENCES

[1] Ai-Wen Luo, Qing-Ming Yi, Min Shi, "Design and Implementation of Area-optimized AES-Based on FPGA", 978-1-61284-109-0/11/2011 IEEE.

[2] JignaeshR.Patel, Rajesh S.Bansode, VikasKaul,"Hybrid security algorithm for data transmission using AES-DES",.IJAIS-2012.

[3] Y.Ou ,C.Sur , K. H Rhee"Region based selective Encryption for Medical Imaging",1st Annual International Workshop-2007

[4] S. H Kamali, R.Shakerian, M.Hedayati,"A new modified version of Advanced Encryption Standard based algorithm for image encryption",International Conference on Electronics and information Engineering, ICEIE-2010.

[5] Ju-Young Oh, Dong-II Yang PhD and ki-Hwan Cho,"A selective Encryption Algorithm based on AES for medical Information",Healthcare informatics research-2010

[6] M.Zeghid ,M.Machhout,L.Khriji,A.Baganne and R.Tourki,"A modified AES based algorithm for image encryption",International journal of computer electrical, Automation, Control and information engineering- 2007.

[7] Mr. Atul M. Borkar, Dr. R. V. Kshirsagar, Mrs. M. V. Vyawahare" FPGA Implementation of AES Algorithm", IEEE-2011, Volume : 3,pp 401-405.

[8] Monica Lib eratori, Fernando Otero, J. C. Bonadero, Jorge Castifieira"AES-128 cipher. high speed, low cost fpga implementation", IEEE-2007.

[9] Chi-Wu Huang, Chi-Jeng Chang, Mao-Yuan Lin, Hung-Yun Tai, "Compact FPGA Implementationof 32-bits AES Algorithm Using Block RAM", IEEE-2007.

[10] Hazim Kamal Ansari, AsadSuhailFarooqi,"Design Of High Speed Uart For Programming Fpga",International Journal Of Engineering And Computer ScienceVolume1 Issue 1 Oct 2012 Page No. 28-36.

[11] Ai-Wen Luo, Qing-Ming Yi, Min Shi, "Design and Implementation of Area-optimized AES-Based on FPGA", 978-1-61284-109-0/11/2011 IEEE.

[12]C. Sivakumar and A .Velmurugan,(2007)"High Speed VLSI Design CCMP AES Cipher for WLAN (IEEE 802.11i)", IEEE, pp398 – 403

[13] Mr. Atul M. Borkar, Dr. R. V. Kshirsagar, Mrs. M. V. Vyawahare,(2011)" FPGA Implementation of AES Algorithm", IEEE, Volume : 3,pp 401-405. [23]G

[14]Yulin Zhang, Xinggang Wang, (2010)"Pipelined Implementation of AES Encryption Based on FPGA", IEEE,pp170 - 173.

[15]Monica Liberatori, Fernando Otero, J. C. Bonadero, Jorge Castifieira,(2007)"AES-128 cipher. high speed, low cost fpga implementation", IEEE