AN APPROACH FOR SECURED INFORMATION TRANSMISSION - AES ALGORITHM IMPLEMENTATION ON FPGA FOR WIRELESS APPLICATIONS

Gira Aparna
Research Scholar, ECE Department,
UCOE, Osmania University, Hyderabad.
aparnaece27@gmail.com

Dr. G.Anitha Mary
Assistant Professor, Loyola Academy,
Degree and PG college, Alwal,
Hyderabad.
anitha.mary@loyalaacademy.edu.in

Dr.Gollapalli Sumana
Programmer, Command Control Center,
Sri Padmavati Mahila Visvavidyalayam,
Tirupati. Andhra Pradesh.
sumana@spmvv.ac.in

G.Sirisha
Assistant Professor, Loyola Academy,
Degree and PG college, Alwal,
Hyderabad.
siribdj.24@gmail.com

Abstract:

The development of the security layers between the wireless terminals is one of the biggest trends in wireless communications. This study emphasizes that wireless communication system for secured data transfer can be done by Bluetooth connectivity. FPGA implementation allows the solution of quadratic programs occurring in MPC at very high speed. This paper presents the development of secure wireless connection terminals on a field programmable gate array (FPGA).The wireless connection has been established using Bluetooth technology and the initialization of a secure algorithm for data exchange is implemented using the advanced encryption standards (AES).The Advanced Encryption Standards (AES) algorithm is used in order to provide the security to the data. This paper analyzes the development of fully secured wireless connection terminals on a FPGA where connection is established using Bluetooth technology and an advanced encryption standard (AES) for encryption and decryption is used to initialize the secured algorithm for data exchange. The proposed system has been validated and demonstrated using the application which involves the encryption and decryption of data and evaluated in terms of resources used and throughput obtained. The proposed system has been validated and demonstrated using an image processing application which involves the encryption and decryption of acquired images from the RC10 FPGA prototyping board's camera

1. INTRODUCTION

1.1 Wireless Communication Techniques:

The data transfer was done mainly by two media- Guided media and unguided media. Guided media can also be termed as wired media where medium is very important issue. Few examples of wired media are twisted pair cable(s), co-axial cable(s), fiber optic cable(s) etc. Wireless transmission, however, due to its broadcast nature inherently develops errors. Most of the transmission errors result because of data collision and channel fading. Broadly the Forward Error Correction (FEC) and Automatic Repeat Request (ARQ) are two major

schemes of transmission error correction over wireless network. Error Correcting Control is very important in modern communication systems. Two correcting codes that are BCH and RS codes are being widely used in satellite communications, computer networks, and magnetic and also optic storage systems. This technology has been designed and intensively used for portable devices where power consumption is an important issue to be addressed. Bluetooth processors are designed to be in low range in terms of power consumption and there is a high demand for this type of processors for operation. Reconfigurable hardware (RH) in the form of field programmable gate arrays (FPGAs) can be an ideal candidate to embed this technology for wireless communication applications. FPGAs are widely used in digital signal processing and communication systems. The advantages offered by FPGAs, such as massive parallelism capabilities, multimillion gate counts, and special low power packages can reduce the amount of memory used, computational complexity and power consumptionAs technology progresses, various sectors like medical industries for blood pressure monitoring, banking, highly confidential applications etc. demands high amount of security regarding data transmission. So in such applications instead of wired transmission, Bluetooth, aiming wireless transmission can be used efficiently to provide highly secured data transmission over wireless link.

As technology progresses, various sectors like medical industries for blood pressure monitoring, banking, highly confidential applications etc. demands high amount of security regarding data transmission. So in such applications instead of wired transmission, Bluetooth, aiming wireless transmission can be used efficiently to provide highly secured data transmission over wireless link

2. PROPOSED SYSTEM

FPGA processes the acquired data and operates as the base station of the transferred data. The prototyping board has been used for testing and evaluating the implemented system. It is equipped with the Xilinx Spartan-III-XC3S250E-4PQ208 FPGA chip. Bluetooth connection has been established using the Bluetooth Module-HC-O5 on both transmitting and receiving terminals. At the receiving section, the data is decrypted using decryption algorithm. Figure 1 below show the block diagram of the proposed system the transmitter and the receiver modules.

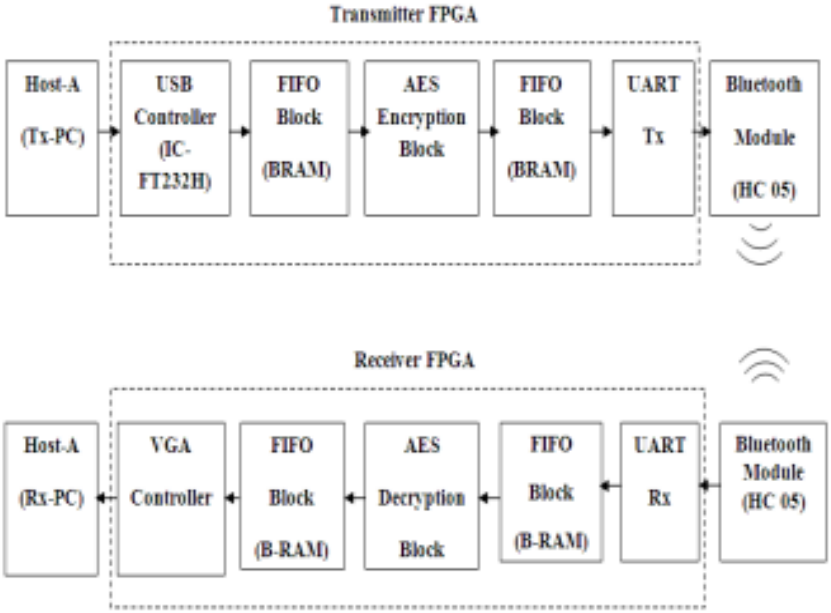

Figure 1: Block Diagram of Implemented System

Two controllers are used at the transmitter section and two more are used at the receiver section of FPGA. The size of one B-RAM is 2048 bytes. So if the size of an image is increased, then number of B-RAM is increased. This FIFO block is used to match the speed of the two devices attached on both the sides. The maximum storage capacity of FIFO block is 15000 bytes. So if any image more than 15000 bytes is taken for the transmission purpose then overwriting of data will take place. Then AES algorithm is used to transmit the data securely using Bluetooth connectivity to the receiver block.

2.1 Encryption Algorithm

The AES algorithm consists of ten rounds of encryption and each round includes four transformations using the corresponding cipher key to ensure the security of the encryption. Output of one round is forwarded to next round and after final round; the cipher text is available which the output of encryption process is. Figure 2 represents the flow diagram of the encryption algorithm.

Figure 2: Flow Diagram of the Encryption algorithm

2.2 Decryption Algorithm:

Decryption process is the exactly reverse process of the encryption process. The stream of 15000 bytes cipher text is received in the receiver block via wireless communication media. and after reception at the receiver section, the data i.e. Cipher text undergoes decryption process. All the transformations in decryption algorithm are executed one after another and the output of first round is forwarded to the next round in the form of input and finally after the last round, final plaintext is available which are the output of decryption process and the exact similar input of encryption process.

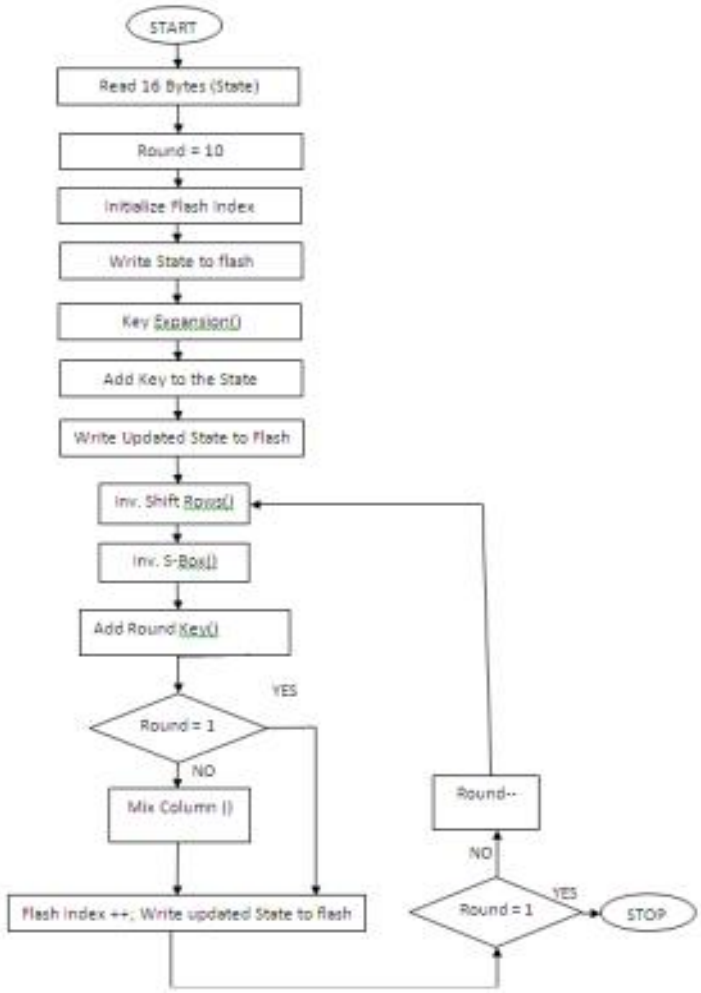

Figure 3: Flow Diagram of Decryption algorithm

3. RESULTS ANALYSIS

Table 1: The hardware utilization of the transmitter, receiver and the image capture

Resources	Transmitter		Receiver		Image Capture	
	Used	Percentage (%)	Used	Percentage (%)	Used	Percentage (%)
Slices	2,856	20	5732	41	1236	8
LUTs	4,200	15	7,982	29	929	3
Shift register	15	-	53	-	10	-
BlockRAM	-	0	36	-	100	-
IOBs	20	9	31	14	45	20
GCLK	1	12	1	12	2	25
Peak memory (Mbits)	190	-	197	-	190	-

Max. Frequency (MHz)	**61.5**	**-**	**49.42**	**-**	**58.3**	**-**
Throughput (Gbits/s)	**7.872**	**-**	**6.32**	**-**	**17.9**	**-**
Power consumption (mW)	**141**	**-**	**141**	**-**	**141**	**-**

4. SIMULATION RESULTS

The implementation results obtained can be divided into two parts; the AES based terminals communication and the image capture and storing.The proposed AES encryption implementation has been compared with other existing architectures as illustrated. The proposed system has shown better performance in terms of throughput rate which improves also the power consumption. Figures 5-9 shows the simulation results of the RTL1, RTL2 of encoder, fixed and floating point output of the encoder, the encryption and the decryption process respectively for the various inputs forced so as to the observe the simulated outputs at different time instances.

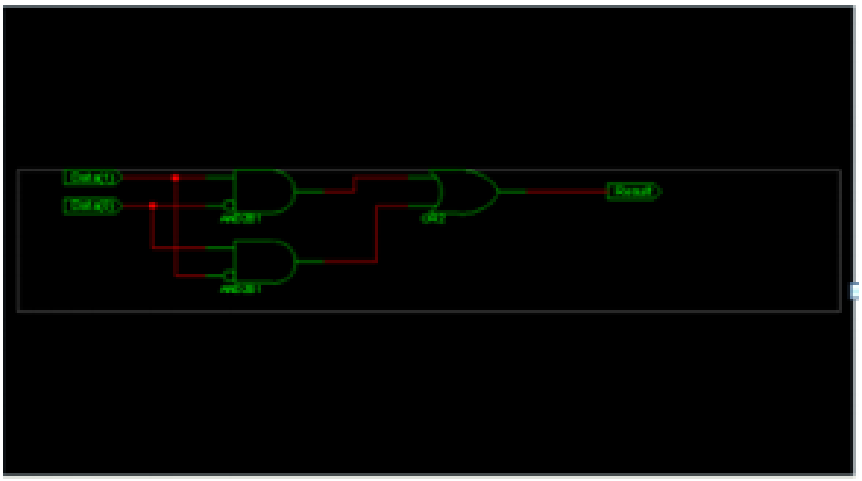

Figure 4: Encoder RTL 1

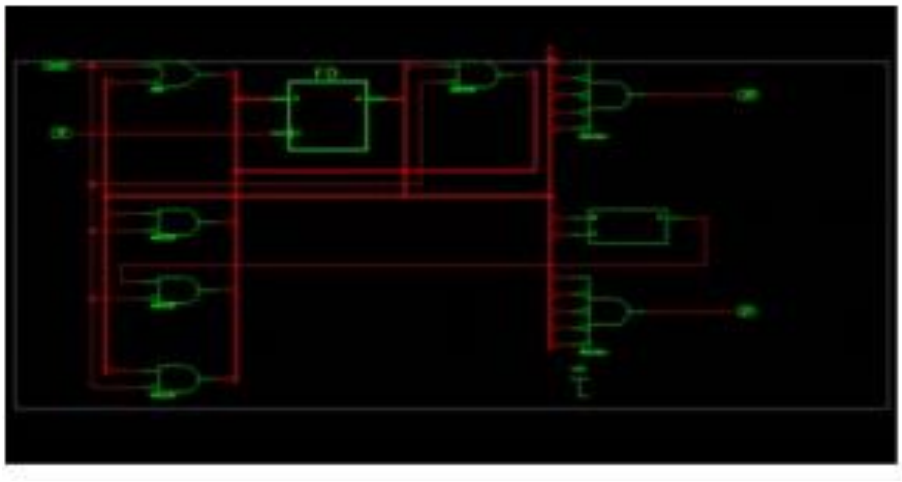

Figure 5: Encoder RTL 2

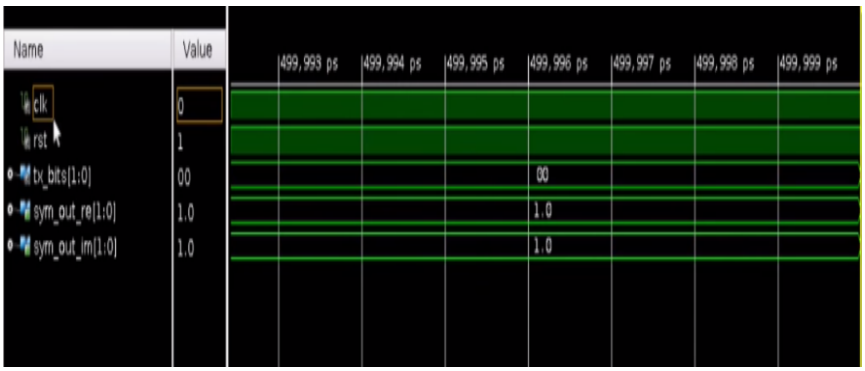

Figure 6: Floating point simulated output of the encoder

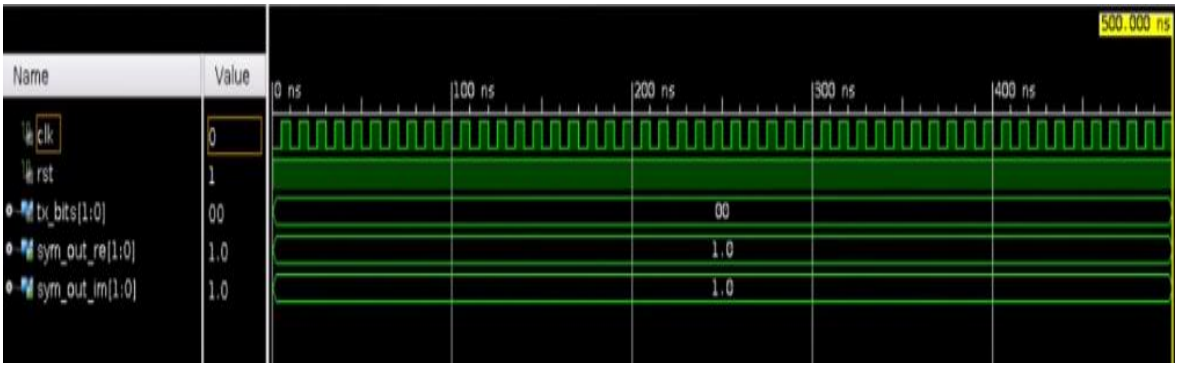

Figure 7: Fixed point simulated output of the encoder

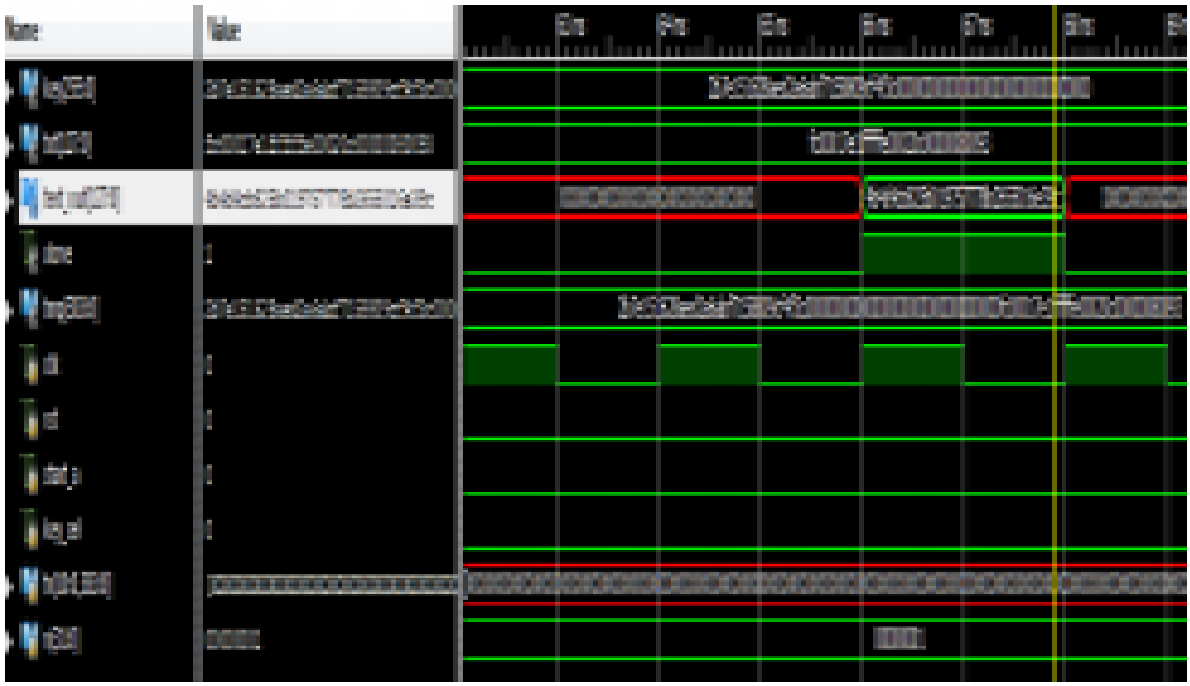

Figure 8: Encryption process

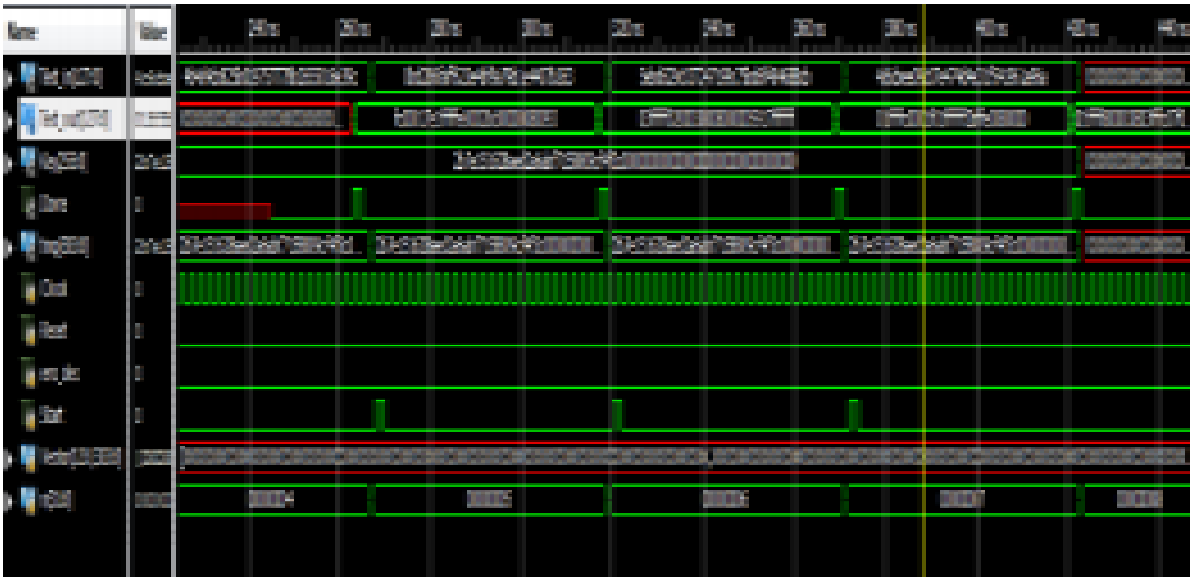

Figure 9: Decryption process

5. CONCLUSIONS

In this paper, high speed design of encoder is proposed for wireless communication based systems. The proposed design has shown an efficient realization of encoder.The system has been evaluated and compared with existing implementations. It shows better results in terms of overall system throughput rate and throughput per slice rate with decrease in chip area thus thereby reducing overall power consumption. The proposed AES encryption implementation has been evaluated and compared with existing implementation. It has shown better results in terms of throughput rate and power consumption which are very important parameters in

wireless communication systems. The scope of the work is for timing analysis and power analysis so as to achieve better performance of the proposed system.

References:

1. HasasnTaha, Abdul N. Sazish, AfandiAhmead, Mhd. Saeed Sharif And Abbes Amira, "Efficient FPGA Implementation of A Wireless Communication System Using Bluetooth Connectivity ", 2010, PP. 1767-1770, IEEE 2010.
2. HuiQin , Tsutomu Sasao and Yukihiro Iguchi. " An FPGA Design Of AES Encryption Circuit with 128-bit keys. In GLSVLSI '05: Proceedings of the 15th ACM Great Lakes Symposium on VLSI, Pages 147-151, 2005.
3. MamtaSood, ManoharWagh, Monika Cheema, "A Review on Various Data Security Techniques in Wireless Communication System", At International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, Vol. 3, Issue 2, pp.883-890, March -April 2013,
4. Sri SuningKusumawardani, Sutopo, "Designing 1 bit Error Correcting Circuit on FPGA Using BCH codes", in proceeding of International Conf. on Electrical, Electronics, Communication, and Information, Jakarta, March 7-8, 2001, pp76-81.
5. G. Rouvroy, F.-X. Standaert, J.-J. Quisquater, and J.-D. Legat. Compact and efficient encryption/decryption module for FPGA implementation of the AES Rijndael very well suited for small embedded applications. In Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on, volume 2, pages 583–587 Vol.2, April 2004.
6. Giacinto Paolo Saggese, AntoninoMazzeo, Nicola Mazzocca, and Antonio G. M. Strollo. An FPGA-based performance analysis of the unrolling, tiling, and pipelining of the AES algorithm. In FPL, pages 292–302, 2003.
7. Ahmed, S.; Sassatelli, G.; Torres, L.; Rouge, L. Survey of New Trends in Industry forProgrammable Hardware: FPGAs, MPPAs, MPSoCs, Structured ASICs, eFPGAs and NewWave of Innovation in FPGAs. In Proceedings of the 2010 International Conference on FieldProgrammable Logic and Applications (FPL), Milano, Italy, 31 August 2010–2 September 2010;pp. 291–297.