Implementation of a Wireless Communication System – A Review

Mamta Sood, PhD.
Head
Department of ECE.
TITC, Bhopal.

Manohar Wagh
M. Tech. (Digital Comm.)
Department of ECE.
TITC, Bhopal.

Monika Cheema
Asst. Prof.
Department of ECE
St. Francis IOT,Bhopal.

ABSTRACT
In early days, the data transfer was done by wired media like co-axial cable(s), fiber optic cable(s) etc. The era has gone. Nowadays wired media is replaced by wireless means, for which Wi-Fi, ZigBee, Bluetooth and Dash7 (Wireless Sensor Networks) are used. Out of these techniques, Bluetooth is mostly used nowadays.

This study emphasizes that wireless communication system for secured data transfer can be done by Bluetooth connectivity. Bluetooth devices are short range and meant for low power utilization, allowing communication between various devices. Various algorithms have been developed for the purpose of providing security to the data to be transferred. Main techniques are DES (Data Encryption Standards), AES (Advanced Encryption Standards), and EES (Escrowed Encryption Standards). Out of them, the Advanced Encryption Standards is the most widely used. This study analyzes the development of fully secured wireless connection terminals on a FPGA where connection is established using Bluetooth technology and advanced encryption standards (AES) are used to initialize the secured algorithm for data exchange. RC-10 Prototyping board with Xilinx Spartan-III XC3S1500L-4-FG320 FPGA device is used for hardware evaluation of system design.

Keywords
Advanced Encryption Standard (AES), Field Programmable Gate Array (FPGA).

1. INTRODUCTION

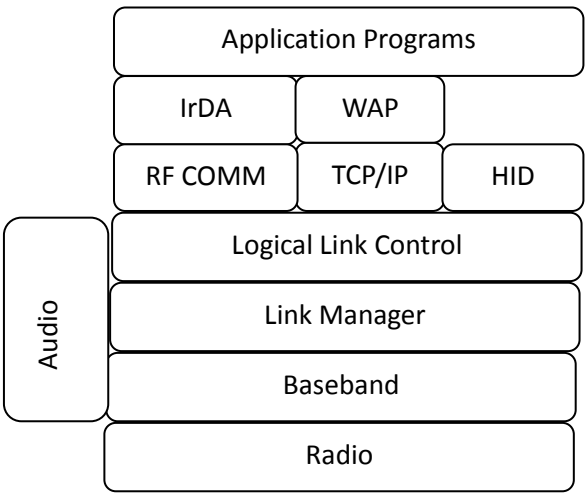
1.1 The Bluetooth Technology
Bluetooth is the wireless communication technology developed in 1998 by Special Interest Group (SIG), to fulfill the demands of Wireless Personal Area Networking (WPAN) [1]. It offers wireless, short distance, point to point and point to multipoint data transfer operating at 2.4 GHz Unlicensed Industrial, Scientific and Medical (ISM) band. By building the Bluetooth into cell phones and a laptop, the cables can be replaced easily [2].

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. [3]. The Bluetooth technology is mainly introduced in portable devices where the least power consumption is needed as well as it acts as a significant tool for the means of wireless communication.

During typical operation a group of devices share a physical radio channel, in which such devices are synchronized to a common clock and frequency hopping pattern. Here mainly the Master-Slave technique is used in which the device acting as the master provides synchronization reference for the provided setup, whereas remaining all other devices acts as slaves working in co-ordination with the master device. A group of devices synchronized in this fashion forms a network which is called as a piconet. This is the fundamental principle behind the Bluetooth communication in the Wireless Technology [1].

Field Programmable Gate Arrays (FPGA) can be used in Digital Signal Processing and Communication Systems providing various advantages like multimillion gate counts, massive parallelism capabilities, in memory reduction, and circuit complexity reduction etc. [4]. Also it is used to design the cryptographic ciphers. Cryptography plays a vital role in providing the control against various security threats. The fading related issues and interference problems can be avoided with the help of fast Frequency Hoping Spread Spectrum (FHSS) Technique.

Fig 1: Bluetooth Protocol Stack [1]



The Bluetooth Protocol Stack which has been implemented by Special Interest Group (SIG) is shown in Fig 1.

From Fig.1, Bluetooth protocol stack consists of various layers. Any Bluetooth system must have the basic protocols like a radio, base band, link manager and logic link control block. The modulated bit streams are then sent and also received with the help of radio protocol. The operations regarding framing, error control, frame control, error correction and detection, timing packet control etc. are performed by means of base band protocol in the Bluetooth protocol stack.

The Link Manger protocol manages states and packets and controls the flow on link. The functions of multiplexing and

Segmentation and Re-assembly (SAR) of larger datagram's into packets are performed by logical link control protocol. All the logical links are created, modified and released by using link manager. In addition to that, all the parameters related to the physical links between the devices are updated by link manager which is achieved with the help of Link Management Protocol (LMP). The link controller encodes and decodes the Bluetooth packets from various parameters related to the physical channel [1].

There are mainly three security levels to provide connectivity between the two devices [5].

- Security Level 1- Identified as a Silent Level. Here the devices won't perform sharing of data. It does not allow the data exchange.
- Security Level 2- Identified as a Private level. Here the device offers maximum security as the device cannot be discovered and thus the data can't be shared between the two devices.
- Security Level 3- Identified as a public level. Here the device can be discovered very easily so as to allow the sharing of data between the two devices and thus it is applicable for all the devices needing the data exchange between them.

1.2 An Overview of Advanced Encryption Standards (AES)

This paper aims at the study of secured data transmission using Bluetooth connectivity and efficient implementation of Advanced Encryption standards (AES).

National Institute of Standards and Technology (NIST) developed a new encryption standard called as Advanced Encryption Standards, in 1997 shortly abbreviated as AES. AES standards are based on algorithmic security, simplicity and it is suitable to both hardware and software implementations. All the above factors are best fitted and supported by Rijndael algorithm, which was developed by Vindert Rijmen and Daemen [6].

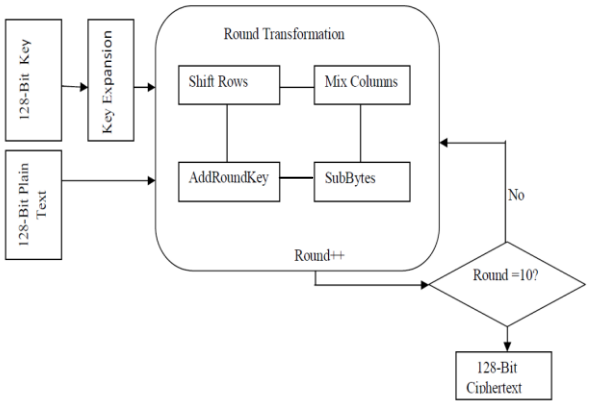


Fig 2: AES 128 Algorithmic Structure

AES operates on fixed-length blocks of data at a time which is known as block cipher and during encryption and decryption, the same key is used which is known as a symmetric key. This key plays a vital role in the data encryption and the data recovery. So, combination is called as a symmetric key block cipher. If such key is not available at the time of decryption, then the original data which is sent along the channel can't be retrieved back into its original format. Fig.2 [7] shows the structure of an Advanced Encryption Standards (AES-128E). Such algorithm is performed on RC-10 prototyping board having Spartan III FPGA chip [7].

2. IMPLEMENTED SYSTEM

The basic block configuration of implemented system is shown in Fig 3. At the transmitter side, the data can be sent to FPGA board. Such data can be text, numbers or the RC-10 CMOS camera is used to take the images. The keyboard controller controls the keyboard and camera controller can be used to control the operations of camera. The select switch is used to select the type of data which can either be text or an image from camera. For secured transmission of data up to receiver block, the data is passed through AES algorithm. The particular data is encrypted; the process is also called as ciphering.

Thereafter the encrypted data is passed to FPGA of receiver block with the help of Bluetooth module. Bluetooth controller controls the Bluetooth module. In short FPGA can be considered to operate as a base station for transferred data. Such a data can also be displayed on host PC-A which can be controlled by UART controller at transmitter FPGA.

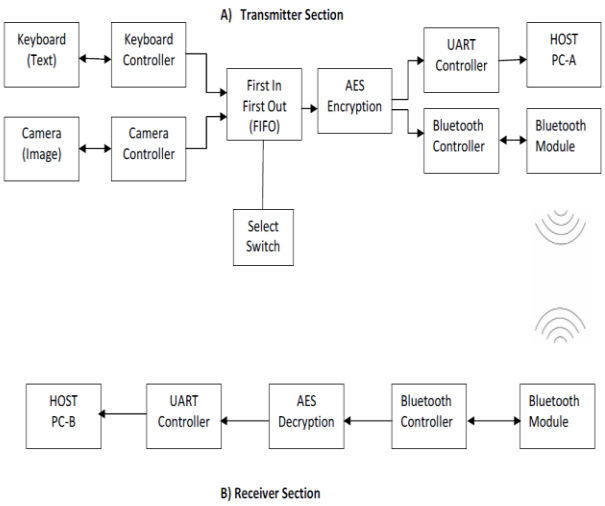
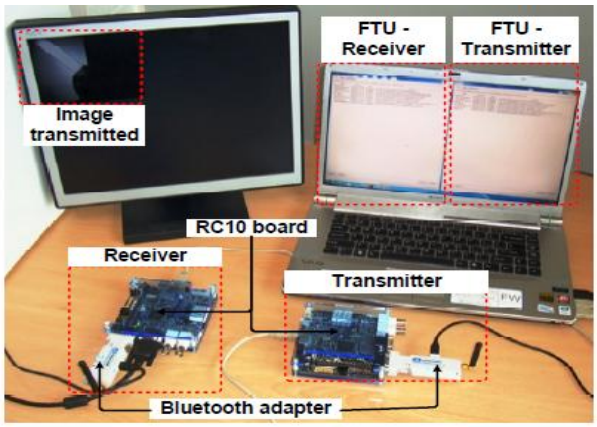


Fig 3: Implemented System

At receiver side the data is again decrypted. The exact reverse operation is performed at the receiver in order to get the data back into the original form. Finally the output data is available at host PC-B of receiver. Also Fig 4 the Bluetooth communication among the two RC-10 FPGA boards can be



studied [8].**Fig 4: Two RC10 FPGA prototyping boards communicating via Bluetooth [8].**

3. FLOW OF OPERATION

Handel-C [9] programming language is used for hardware compilation and implementation of various algorithms. Fig.4 shows the Bluetooth communication between two RC10 FPGA prototyping boards. Here author [Ref.8] has implemented the system by implementing the Bluetooth module onto the FPGA boards at both the sections (i.e. the transmitter and receiver sections). Image was taken through RC10 CMOS camera and was transmitted by using Advanced Encryption standards (AES) algorithms.

From study it is observed that, the system is implemented in three steps. The first implementation step deals with development of Bluetooth connection between two RC-10 prototyping boards, with the help of class-I RS-232 based LM058 adapter [8], the second step is AES algorithm followed by an Image processing part.

3.1 Encryption Process

The process of encryption implemented on FPGA is AES-128 implementation shown in Fig 5.

The data received at AES encryption block undergoes mainly four operations-

Sub-bytes (),

Shift Rows (),

Mix Columns (),

Add Round Key ().

At transmitter section the process called pipelined process is performed. The method is so called because the operations like key expansion and AES-128 transformations are performed simultaneously in order to save clock cycles [5]. The design flow for encryption process at transmitter is shown in Fig 5.

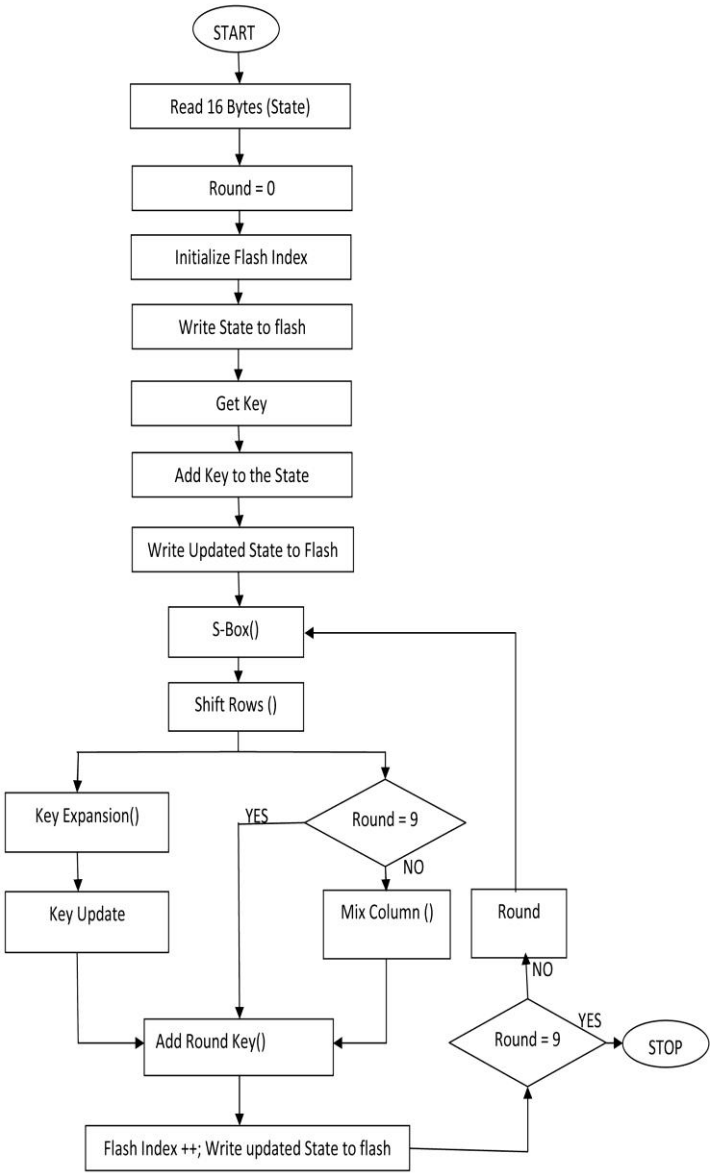


Fig 5: Encryption Design Flow

3.2 Decryption Process

Again the data received at the receiver block undergoes four operations-

Inverse Sub-Bytes (),

Inverse Shift Rows (),

Inverse Mix Columns,

Inverse Add Round Key ().

At receiver section the process called unpipelined process takes place. The process is called so because key expansion and AES decryption are performed one after another [5].

The design flow for decryption process at the receiver is shown in Fig 6.

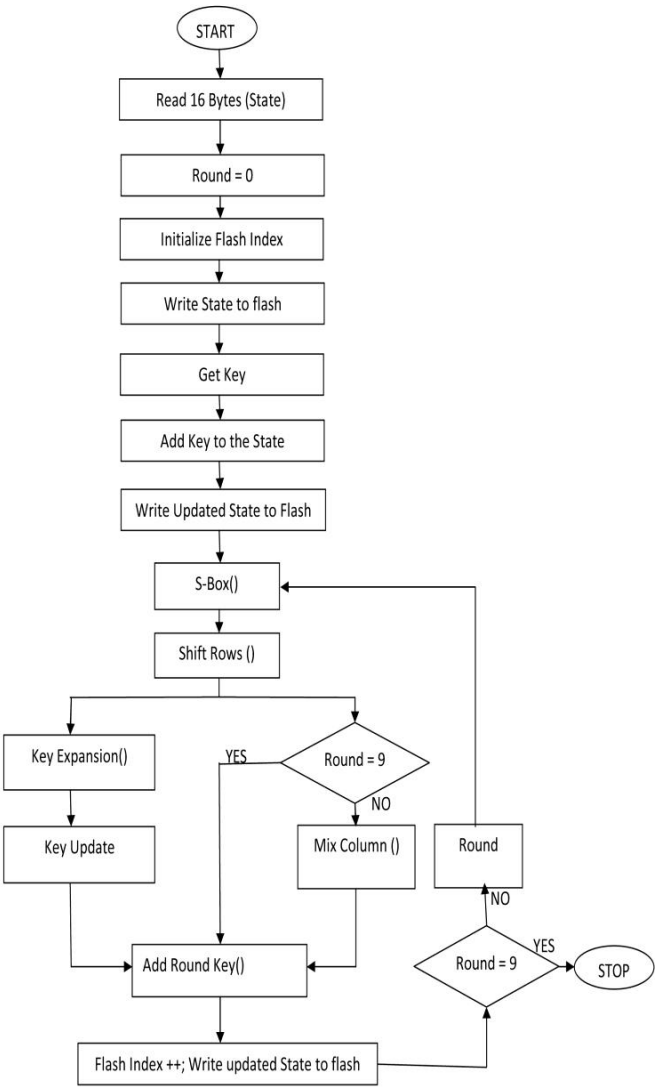


Fig 6: Decryption Design Flow

3.3 Image capture and storing process

The available resources and processing time are very limited so for these reason the process of image capturing and storing is performed separately in different configuration path as given in Fig 7.

Reading the pixel value is the very important task in the process of image capture and image storing.

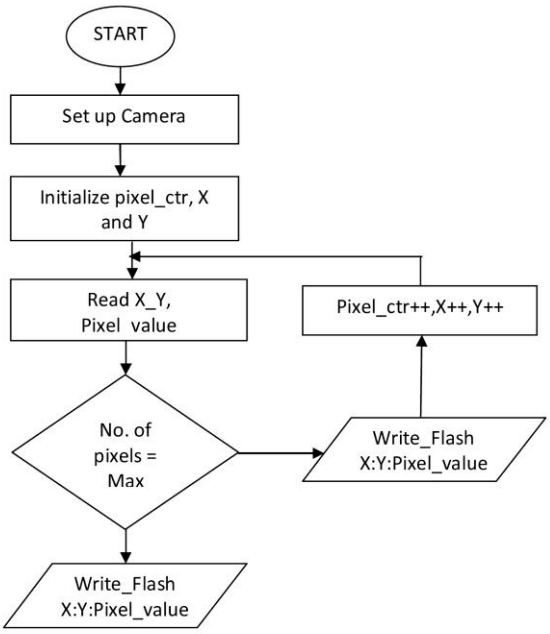


Fig 7: Image Capture Process

4. RESULTS

The study regarding an efficient implementation of AES encryption for wireless communication system has been presented in this paper. The AES algorithm has been implemented to capture, store and transmit frames by camera.

By performing the same operations in [5] Fig. 8 shows FPGA chip layout obtained at the transmitter section [5]. Also the chip layouts observed during decryption process and an image capture process are shown below in Fig. 9[5] and Fig. 10[5] respectively [5].The resources used for implemented system are shown in Table 1[5]. Also Table 2 shows the comparison of AES encryption model with other existing work [5].

For both ciphering and de-ciphering process large number of look up tables have been occupied. The results obtained were very competitive results in terms of throughput per unit slices.

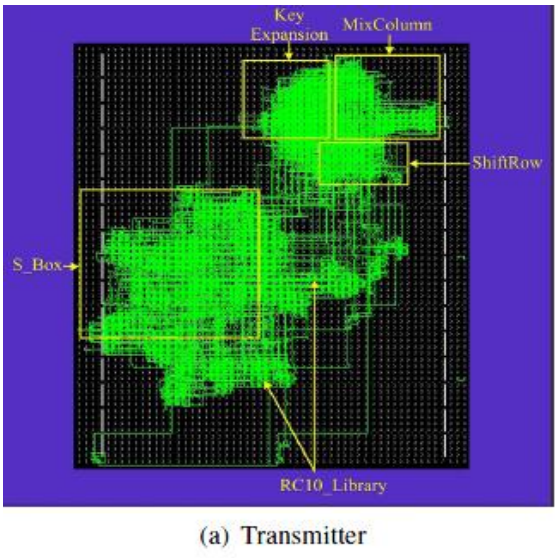
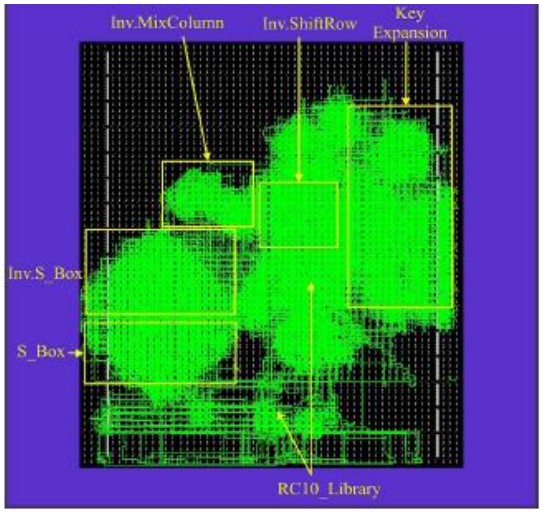
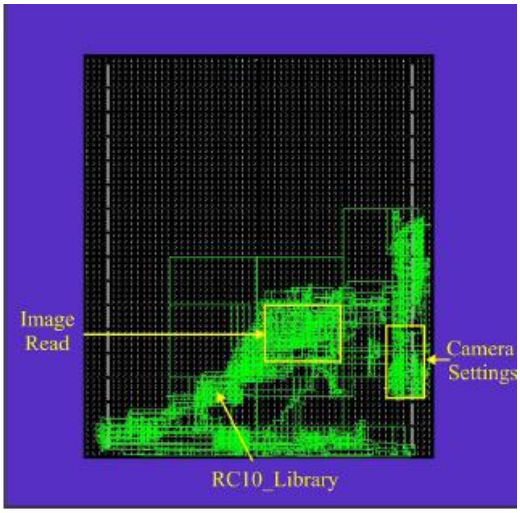


Fig. 8: FPGA Chip Layout at Transmitter [5]



(b) Receiver

Fig. 9: FPGA Chip Layout at Receiver [5]



(c) Image Capture

Fig. 10: FPGA Chip Layout for Image Capture [5]

Table 1: Resources Used For Implemented System [5].

Resources	Transmitter		Receiver		Capture Image	
	Used	Percentage (%)	Used	Percentage (%)	Used	Percentage (%)
Slices	2,546	19	5,457	40	1,065	8
LUTs	4200	15	7,982	29	929	3
Shift Register	15	-	53	-	10	-
Dual Port RAM	8	-	36	-	100	-
Block RAM	-	0	1	32	1	3
IOBs	20	9	31	14	45	20
GCLK	1	12	1	12	2	25
DCM	1	25	1	25	1	25
Peak Memory (Mbits)	190	-	197	-	190	-
Maximum Frequency (MHz)	61.5	-	49.42	-	58.3	-
Throughput (Gbits/s)	7.872	-	6.32	-	17.9	-
Power Consumption (mW)	141	-	141	-	141	-

Table 2: Comparison of Implemented AES encryption Model with Other Models [5].

Design	Device	Slices	Block RAMs	Max freq. (MHz)	Throughput (Gbps)	Throughput/slice (Mbps/slice)
Implemented system	Spartan-III XC3S15001	2,564	N/A	61.5	7.9	3.2
Zambreno et al. [7]	Virtex-II XC2V4000	16,938	N/A	184.1	23.654	1.391
Rouvroy et al.[10]	Spartan-III XC3S50-4	163	3	71	0.208	0.132
Chodowiec & Gaj [11]	Spartan-II XC2S30-6	222	3	60	0.166	0.07
Qin et al. [12]	Altera stratix 1S20C5	5,145	N/A	39.68	5.61	1.12
Jarvinen et al. [13]	Virtex-E XCv1000e-8	5,810	100	158	20.3	1.09
Standaert et al. [14]	Virtex-E XCV 3200e-8	9,446	N/A	169.1	21.64	2.29
Saggesse et al. [15]	Virtex-E XCV 2000e-8	11,719	N/A	129.2	16.5	1.48
Hodjat & verbauwhede [16]	Virtex-II Pro-XC2VP20	15,112	N/A	145	18.56	1.228

5. SUMMARY AND FUTURE SCOPE OF WORK

This study aimed at efficient re-configurable wireless communication systems using FPGAs and Bluetooth connectivity. The RC-10 FPGA prototyping boards were used to demonstrate the implemented system. AES encryption was also evaluated and compared with existing implementations and finally the better results regarding throughput rate and power consumption were obtained. By using less number of slices, the better throughput per slice can be achieved as compared to the previous existing techniques.

After studying this paper, this system can be implemented in CCTV Cameras to provide real time coverage through wireless media using Bluetooth connectivity in future. By collecting the continuous live coverage of various activities inside the bank, the live coverage can be sent to through wireless means. This implemented system can be taken as the reference for further work and moving pictures or video can be sent in real time manner.

6. REFERENCES

[1] Bluetooth Special Interest Group, The Bluetooth System: Part-B: Baseband Specification Draft Ver 1.1, (2000).

[2] Sunhee Kim and Seungjun LEE, " Design of Bluetooth Baseband Controller Using FPGA", in Journal of Korean Physical Society, vol.42:200-205, Feb.

[3] Youquan Zheng and Zhenming Feng, "Simplification of Bluetooth Radio Devices", in networked appliances, 2002. G. AITHER S BURG Proceedings 2002 IEEE 4th International Workshop, Pages 107-115, 2002.

[4] Lanping Deng, K. Sobti and C. Chakraborty, "Accurate models for estimating area and power of FPGA Implementations. In Acoustic, Speech and Signal Processing, 2008. ICA SSP 2008. IEEE International Conference on Pages 1417-1420, 31-2008-April-4 2008.

[5] Hasasn Taha, Abdul N. Sazish, Afandi Ahmead , Mhd. Saeed Sharif and Abbes Amira, " Efficient FPGA Implementation of a wireless Communication System Using Bluetooth Connectivity ", IEEE-2010, PP. 1767-1770.

[6] J. Daemen and V. Rijmen, " The Block Cipher Rijndael;," Lecture Notes In Computer Science, Vol.1820/2000, pp. 277-284.

[7] Joseph Zambreno, David Nguyen and Alok Chaudhary. Exploring Area/ Delay Tradeoffs in an AES FPGA Implementation. In Proceedings of the 14th Annual International Confernce on FPLA (Pages 575-585. Springer 2004).

[8] Anurag Gupta, Afandi Ahmadd,, Mhd Saeed Sharif And Abbes Amira, " Rapid Prototyping of AES Encryption For Wireless Communication System On FPGA".

[9] [online] available on : http://www.mentor..com/

[10] 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.v. Proceedings. ITCC 2004., International Conference on, volume 2, pages 583-587. April 2004.

[11] Powel Chodoweic and Kris Gag. Very Compact FPGA Implementation of AES Algorithm. Cryptographic Hardware And Embedded Systems-CHES -2003, 2779:319-333, Oct. 2003.

[12] Hui Qin , 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.

[13] Kimmo U. Jarvinen, Matti T. Tommiska, and Jorma O. Skytta. A fully pipelines memory less 17.8 GBPS AES-128 Encryptor. In FPGA '03: Proceedings of the 2003 ACM/CIGDA eleventh International Symposium On Field Programmable Gate Arrays, Pages 207-215, New York, NY, USA, 2003. ACM.

[14] Francois-Xavier Standaert, Gael Rouvroy, Jean- Jacques Quisquater and Jean Didier Legat. Efficient Implementation Of Rijndael Encryption In Reconfigurable Hardware And Embedded Systems-CHES 2003, Pages 334-350, May 2003.

[15] Giacinto Paolo Saggase, Antonino Mazzeo, Nicola Mazzocca And Antonio G.M. STROLLO. An FPGA-Based Performance Of The Unrolling, Tiling And Pipelining Of The AES-Algorithm. In FPL, Pages 292-302,2003.

[16] A. Hodjat and I. Verbauwhede. A 21.54 GBPS Fully Pipelined AES Processor on FPGA. In FCCM, 2004. 12th Annual IEEE Symposium On, Pgs 309-09,2004.