Efficient FPGA implementation of a wireless communication system using Bluetooth connectivity

Conference Paper · July 2010

DOI: 10.1109/ISCAS.2010.5537610 · Source: IEEE Xplore

5 authors, including:

Afandi Ahmad
Universiti Tun Hussein Onn Malaysia
41 PUBLICATIONS **153** CITATIONS

Efficient FPGA Implementation of a Wireless Communication System Using Bluetooth Connectivity

Hasan Taha, Abdul N. Sazish, Afandi Ahmad, Mhd Saeed Sharif, and Abbes Amira*
Electronic and Computer Engineering
School of Engineering and Design
Brunel University, West London, United Kingdom
*Email: abbes.amira@brunel.ac.uk

***Abstract*— The development of the security layers between the wireless terminals is one of the biggest trends in wireless communications. Bluetooth can be described as the short range and the low power supplements that holds the connection protocol through various devices. This paper presents the development of a secure wireless connection terminals on a field programmable gate array (FPGA). The wireless connection has been established using Bluetooth technology and the initialisation of a secure algorithm for data exchange is implemented using the advanced encryption standards (AES). The proposed system has been validated and demonstrated using using an image processing application which involves the encryption and decryption of acquired images from the RC10 FPGA prototyping board's camera.The evaluation of different building block has been carried out in terms of area, resources used and power consumption.**

I. Introduction

A new wireless communication technology named Bluetooth had been introduced by the special interest group (SIG) in 1998 [1]. Bluetooth connectivity offers short distance, point to multipoint data exchange. It operates over the unlicensed band with a carrier frequency of 2.4 GHz which is industrial, scientific and medical (ISM) band [1]. Bluetooth applications have been targeted towards portable devices like personal digital assistants (PDA)s, laptops, mobiles ...etc.

The SIG proposed architecture was a substitution of a wired connection with short range limits of transmission for audio, video, and other data formats. Bluetooth technology is not only a hardware motivation, it is also a software compatibility, a protocol stack that has been defined by the SIG with layers as shown in Fig. 1.

Bluetooth radio system employs frequency hopping spread spectrum (FHSS) techniques to avoid interference with other devices. Each Bluetooth device is able to hop on 79 channels, using single channel at a time. Hopping with 625 microseconds between channels resulted in making 1600 hops per second. Another modulation techniques applied like adaptive frequency hopping (AFD) introduced with Bluetooth 1.2 specifications [3].

The connectivity of the devices can be classified into three security levels or modes [4]:

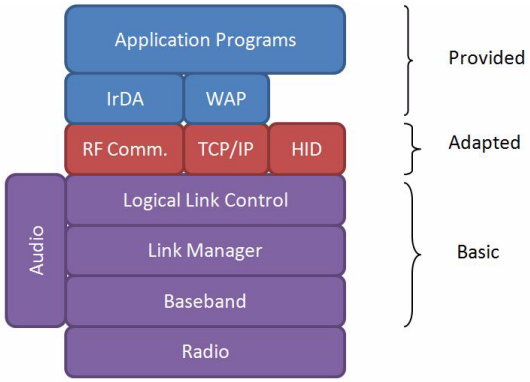


Fig. 1. Bluetooth Stack Protocol [2]

- Mode 1 (Silent): the device will never accept or share any connections
- Mode 2 (Private): is a non-discoverable device
- Mode 3 (Public): is a discoverable device

Bluetooth devices can be classified into five levels [4], trusted, untrusted, authenticated, unauthenticated and Unknown. These devices can be attacked in many forms such as BlueSnarfing, Service Theft, Denial of Service, BlueJacking, BluePrinting and BlueBugging.

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 [5]. 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 consumption. This flexibility in design allows introducing several algorithms for a specific purpose and gives selective decisions that depend

978-1-4244-5309-2/10/$26.00 ©2010 IEEE

upon the simulated results.

The aim of this paper is to develop a reconfigurable environment for secure data transmission using Bluetooth connectivity. An efficient implementation of the advanced encryption standards (AES) algorithm has been carried out on the RC10 prototyping board equipped with Spartan 3 FPGA chip. The proposed system has been also demonstrated through secure transmission of the digital images acquired using the RC10 embedded camera.

The rest of the paper is organised as follows. The proposed system architecture is presented in section II. The FPGA implementation is described in section III. Results and analysis are presented in section IV. Concluding remarks are given in Section V.

II. Proposed System

The transmitter block obtains its data which can be numbers, text or images acquired using the RC10 CMOS camera. AES algorithm is then used to securely transmit the data using Bluetooth connectivity to the receiver block. The file transfer utility (FTU), host application is used to configure the FPGA with the corresponding bitstream files for configuring the transmitter, receiver, and AES execution. Fig. 2 shows the proposed system with its main building blocks.

FPGA processes the acquired data and operates as the base station of the transferred data. The RC10 prototyping board has been used for testing and evaluating the proposed system [6]. It is equipped with the Xilinx Spartan 3 XC3S1500L-4-FG320 FPGA chip, and supported with different peripherals to suit a range of applications. Bluetooth connection has been established using the LM058 serial to Bluetooth adapters on both transmitting and receiving terminals.

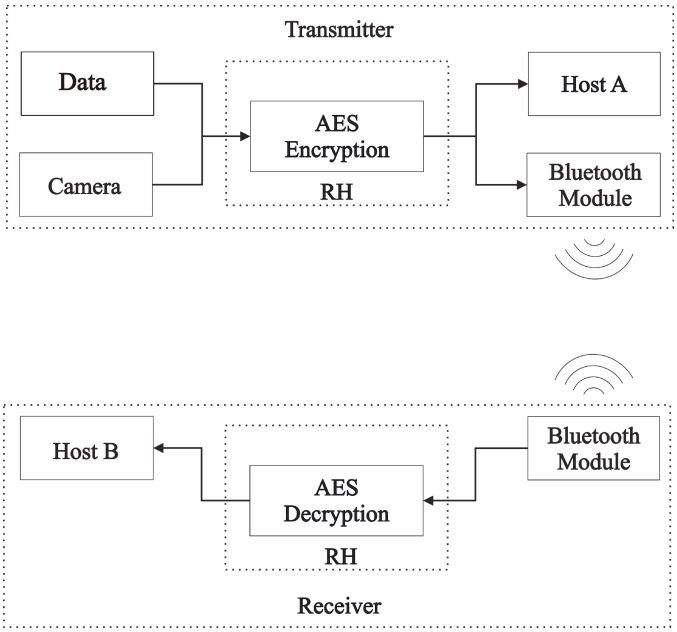


Fig. 2. Proposed system block diagram

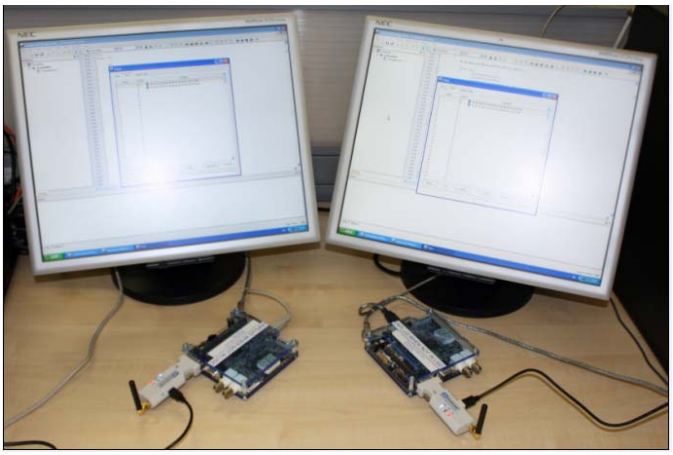


Fig. 3. RC10 FPGA boards communicating via Bluetooth

III. FPGA Implementation

The first step of the implementation is concerned with the development of a Bluetooth connection between two the RC10 boards; then followed by AES algorithm implementation (AES-128) and image processing. Fig. 3 shows the proposed reconfigurable environment using FPGA and Bluetooth connectivity. Handel-C [6] programming language has been used for hardware compilation and efficient implementation of different tasks and algorithms.

A. Encryption

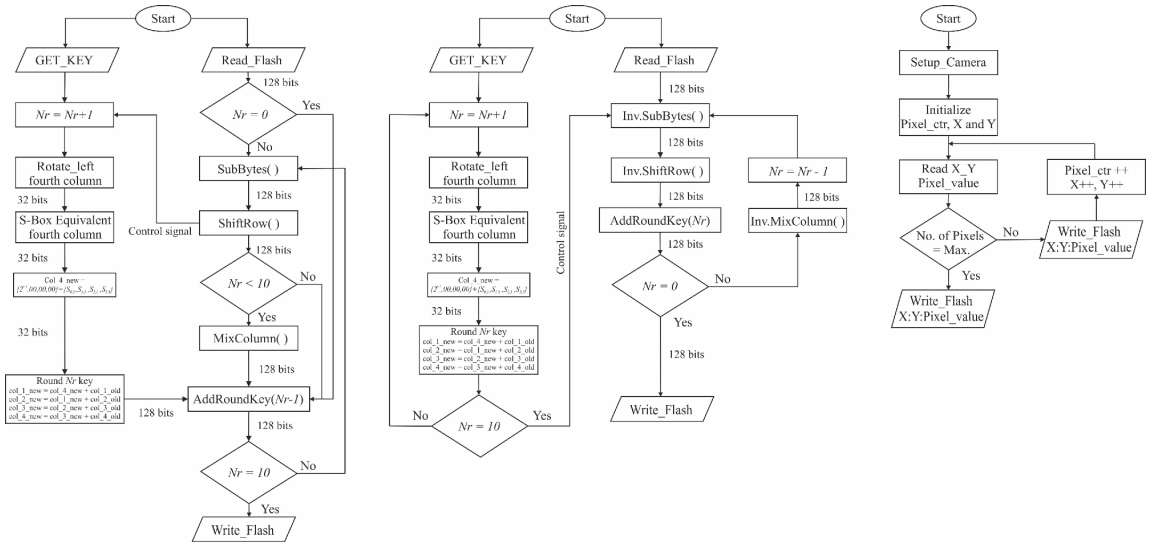
AES encryption block processes the incoming data using four main basic operations SubBytes( ), ShiftRows( ), MixColumns( ), and AddRoundKey( ). The key expansion processed at the same time with the AES transformations, in order to conserve the clock cycle which is called the *Pipelined* method. Fig. 4 (a) shows the transmitter encryption design flow.

B. Decryption

The decryption process is performed using the following functions: Inv.SubBytes( ), Inv.ShiftRow( ), AddRoundKey( ), and Inv.MixColumn( ) respectively. In different way from the encryption method, decryption processes the Key expansion algorithm before starting the AES deciphering. This is because the round key arrays interact in descending order with the AES algorithm. Fig. 4 (b) shows the decryption design flow with *UnPipelined* method.

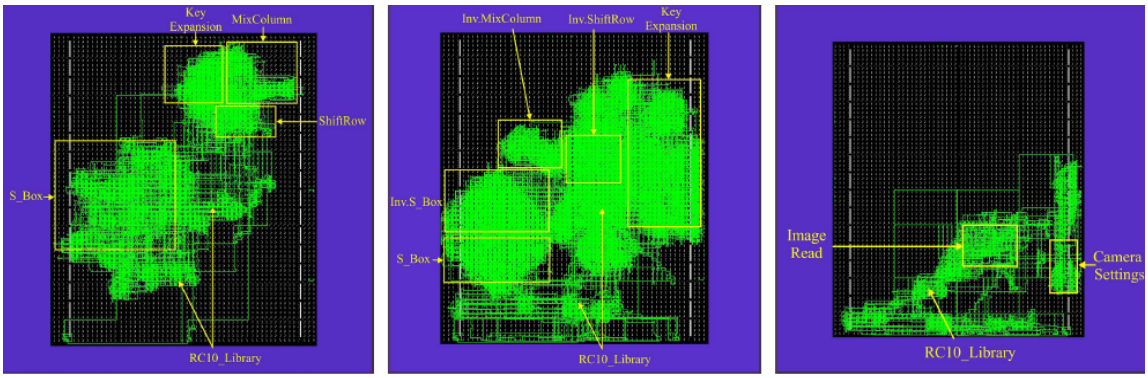
C. Image Capturing and Storing

The second part of the system implementation is the image processing. Due to the limitations of the available resources and processing time, the image manipulation algorithm is configured separately on the FPGA in different configuration path. The design flow of image capturing is shown in Fig. 4 (c).



(a) Encryption (b) Decryption (c) Image Capture

Fig. 4. AES design flow



(a) Transmitter (b) Receiver (c) Image Capture

Fig. 5. FPGA chip layouts

TABLE I
RESOURCES USED FOR THE PROPOSED SYSTEMS

Resources	Transmitter		Receiver		Image Capture	
	Used	Percentage (%)	Used	Percentage (%)	Used	Percentage (%)
Slices	2,546	19	5,457	40	1,065	8
LUTs	4,200	15	7,982	29	929	3
Shift register	15	-	53	-	10	-
Dual port RAM	8	-	36	-	100	-
BlockRAM	-	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	-
Max. Frequency (MHz)	61.5	-	49.42	-	58.3	-
Throughput (Gbits/s)	7.872	-	6.32	-	17.9	-
Power consumption (mW)	141	-	141	-	141	-

TABLE II
COMPARISON OF AES ENCRYPTION MODEL WITH OTHER EXISTING WORK

Design	Device	Slices	BlockRAMs	Max. Freq. (MHz)	Throughput (Gbps)	Throughput/Slice (Mbps/slice)
Proposed System	Spartan-III XC3S1500l	2,564	N/A	61.5	7.9	3.2
Rouvroy et al. [7]	Spartan-III XC3S50-4	163	3	71	0.208	0.132
Chodowiec & Gaj [8]	Spartan-II XC2S30-6	222	3	60	0.166	0.07
Qin et al. [9]	Altera Stratix 1S20C5	5,145	N/A	39.68	5.61	1.12
Jarvinen et al. [10]	Virtex-E XCV1000e-8	5,810	100	158	20.3	1.09
Standaert et al. [11]	Virtex-E XCV3200e-8	9,446	N/A	169.1	21.64	2.29
Saggesse et al. [12]	Virtex-E XCV2000e-8	11,719	N/A	129.2	16.5	1.48
Hodjat & Verbauwhede [13]	Virtex-II Pro-XC2VP20	15,112	N/A	145	18.56	1.228
Zambreno et al. [14]	Virtex-II XC2V4000	16,938	N/A	184.1	23.654	1.391

IV. RESULTS AND ANALYSIS

The implementation results obtained can be divided into two parts; the AES based terminals communication and the image capture and storing. Fig. 5 shows the internal implementation of the FPGAs' mapping. It is worth mentioning that a large number of look up tables (LUTs) is consumed by the S-Box function at the transmitter as illustrated in Fig. 5 (a). The LUTs usage is justified by the implementation of the S-Box function using tables that consist of 256 byte with a conditional access which gives a total of 900 LUTs. Beside the S-Box LUTs the Inv.S-Box and Key Expansion functions made the receiver to allocate higher number of LUTs as shown in Fig. 5 (b). Table I shows the resources used for the proposed system. The proposed AES encryption implementation has been compared with other existing architectures as illustrated in Table II. The proposed system has shown better performance in terms of throughput rate which improves also the power consumption.

V. CONCLUSIONS

An efficient reconfigurable wireless communication system has been presented in this paper using FPGAs and Bluetooth connectivity. AES algorithm has been implemented for secure data transmission between the two terminals. The RC10 FPGA prototyping boards have been used to demonstrate and validate the proposed system. 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 Bluetooth based wireless communication systems.

REFERENCES

[1] R. Shorey and B.A. Miller. The Bluetooth technology: merits and limitations. In *Personal Wireless Communications, 2000 IEEE International Conference on*, pages 80–84, 2000.

[2] S. Kim and S. Lee. Design of Bluetooth baseband controller using FPGA. *Journal of the Korean Physical Society*, 42:200–205, Feb. 2003.

[3] Youquan Zheng and Zhenming Feng. Simplifications of the Bluetooth radio devices. In *Networked Appliances, 2002. Gaithersburg. Proceedings. 2002 IEEE 4th International Workshop on*, pages 107–115, 2002.

[4] Ma Kui and Cao Xiuying. Research of Bluetooth security manager. In *Neural Networks and Signal Processing, 2003. Proceedings of the 2003 International Conference on*, volume 2, pages 1681–1684, Dec. 2003.

[5] Lanping Deng, K. Sobti, and C. Chakrabarti. Accurate models for estimating area and power of fpga implementations. In *Acoustics, Speech and Signal Processing, 2008. ICASSP 2008. IEEE International Conference on*, pages 1417–1420, 31 2008-April 4 2008.

[6]

[7] 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.

[8] Pawel Chodowiec and Kris Gaj. Very compact FPGA implementation of the AES algorithm. *Cryptographic Hardware and Embedded Systems - CHES 2003*, 2779:319–333, Oct. 2003.

[9] Hui Qin, Tsutomu Sasao, and Yukihiro Iguchi. An FPGA design of AES encryption circuit with 128-bit keys. In *GLSVSLI '05: Proceedings of the 15th ACM Great Lakes symposium on VLSI*, pages 147–151, 2005.

[10] Kimmo U. Järvinen, Matti T. Tommiska, and Jorma O. Skyttä. A fully pipelined memoryless 17.8 gbps AES-128 encryptor. In FPGA *'03: Proceedings of the 2003 ACM/SIGDA eleventh international symposium on Field programmable gate arrays*, pages 207–215, New York, NY, USA, 2003. ACM.

[11] Francois-Xavier Standaert, Gael Rouvroy, Jean-Jacques Quisquater, and Jean-Didier Legat. Efficient implementation of Rijndael encryption in reconfigurable hardware: Improvements and design tradeoffs. *Cryptographic Hardware and Embedded Systems - CHES 2003*, pages 334–350, May 2003.

[12] Giacinto Paolo Saggese, Antonino Mazzeo, 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.

[13] A. Hodjat and I. Verbauwhede. A 21.54 gbits/s fully pipelined AES processor on FPGA. In *Field-Programmable Custom Computing Machines, 2004. FCCM 2004. 12th Annual IEEE Symposium on*, pages 308–309, April 2004.

[14] Joseph Zambreno, David Nguyen, and Alok Choudhary. Exploring area/delay tradeoffs in an AES FPGA implementation. In *In Proceedings of the 14th Annual International Conference on Field-Programmable Logic and Applications (FPL 04*, pages 575–585. Springer, 2004.