Fpga Secured Wireless Communication Using Aes

Mr.Rahane M.D[1], Prof.Turkane S.M.[2]

[1]*ME Electronics & Telecommunication Engineering Pravara Rural Engineering College Loni (MS), 413736*
[2]*Asst.Prof. Electronics & Telecommunication Engineering Pravara Rural Engineering College Loni (MS), 413736*

Abstract

Now a day's wireless secure communication is the main aspect in network applications development. Earlier technologies like Bluetooth with secure communication using secure wireless connection terminals on a field programmable gate array (FPGA) gives most efficient secure communication in wireless networks. It has shown better results in terms of throughput rate and power consumption which are very important parameters in Bluetooth based wireless communication systems. In this techniques cost and speed are the two main factors in communication for wireless techniques. This paper presents a compact implementation of advanced encryption standard AES using different devices of FPGA technology. This implementation can be carried out through several trade-off between area and speed.

Index Terms: *FPGA, AES, cryptography, VHDL, compact encryption / decryption implementation, embedded systems.*

I. INTRODUCTION

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. Hardware implementations of the Advanced Encryption Standard (AES) Rijndael algorithm have recently been the object of an intensive evaluation. URING the selection process of the AES [1], an Important criterion was the efficiency of the cipher in different platforms, including FPGAs. Since 2001, various implementations have consequently been proposed, exploring the different possible design tradeoffs ranging from the highest throughput to the smallest area.Each of those implementations usually focuses on a particular understanding of "efficiency". The three major design targets with respect to hardware realization are: optimization for area or cost, low latency that minimizes time to encrypt a single block and high throughput to encrypt multiple blocks in parallel. All these design criteria involve a trade-off between area and speed. There is a wide range of equipment where encryption is needed for authentication and security but throughput is not the principal concern.

A low cost, small area design could be used in smart card applications as well as in other storage devices and low speed communication channels. Customizing the AES algorithm attracted attention of researchers to provide proprietary security. Moreover, the proposed customized AES is incorporated in an encryption unit that is implemented using FPGA. The customization of the AES is designed to cover three main AES cryptographic functions, these are: S-box Generation, Mix Column Transformation, and Key Expansion Function.

The S-Box generation process results in a new S-Box. The new S-Box is tested to be sure of satisfying the required cryptographic features: algebraic degree, non linearity, propagation criteria, correlation immunity, and balancedness.

The customized AES is tested also against statistical randomness properties [1]. Using FPGA, the architecture of the encryption unit is composed of two main units. The first unit is the Proposed Encryption Unit which divided into four main functional block, these are the loop controller module, the encryption and decryption round module, key expansion function module, and the ram module. The second unit is Multi-Rate Unit which composed of four main modules UART module, Clock divider module, Signal Compression module, and Decision module. The proposed AES algorithm can be increased Speed of a network with wireless communication.

II. RELATED WORK

Bluetooth establishes ad-hoc voice and data connections and operates in the 2.4 GHz unlicensed ISM band. Its specification is open and royalty-free. The symbol rate is 1 Ms/s to exploit a maximum available channel bandwidth of 1 MHz. Fast frequency hopping is applied to combat interference and fading. A shaped, binary FM modulation is applied to minimize transceiver complexity.

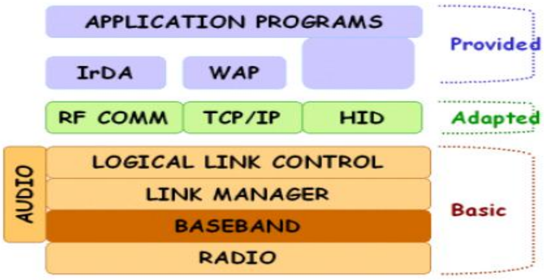

Fig 1: Bluetooth Parameters.

Hardware Design:

The register file is used to exchange information between LM and BB. The controller takes care of timing and state changing, as well as low-level link control. The data path composes the packet to be transmitted and decomposes the received packet. Advanced Encryption Standard (AES), a Federal Information Processing Standard (FIPS), is an approved cryptographic algorithm that can be used to protect electronic data. The AES can be programmed in software or built with pure hardware. However Field Programmable Gate Arrays (FPGAs) offer a quicker and more customizable solution.

In cryptography[2], the AES, also known as Rijndael, is a block cipher adopted as an encryption standard by the US government, which specifies an encryption algorithm capable of protecting sensitive information. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called cipher-text. Decryption of the cipher-text[3] converts the data back into its original form, which is called plaintext.

The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. The hardware implementation of the Rijndael algorithm can provide either high performance or low cost for specific applications.

III. FPGA

Field Programmable Gate Array (FPGA) is an integrated circuit that can be bought off the shelf and reconfigured by designers themselves. With each reconfiguration, which takes only a fraction of a second, an integrated circuit can perform a completely different function. FPGA consists of thousands of universal building blocks, known as configurable logic blocks (CLBs), connected using programmable interconnects. Reconfiguration is able to change a function of each CLB and connections among them, leading to a functionally new digital circuit. For implementing cryptography in hardware, FPGAs provide the only major alternative to custom and semicustom Application Specific Integrated Circuits (ASICs). Integrated circuits that must be designed all the way from the behavioral description to the physical layout are sent for an expensive and time-consuming fabrication.

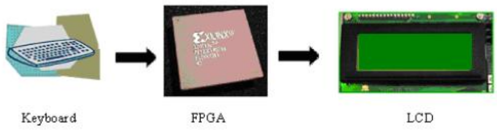

Fig 2: Overall system design

The input and output used by Rijndael at its external interface are considered to be one dimensional arrays of 8-bit bytes numbered upwards from 0 to the 4*Nb-1. These blocks hence have lengths of 16, 24 or 32 bytes and array indices in the ranges 0..15, 0..23 or 0..31. The cipher key is considered to be a one-dimensional arrays of 8-bit bytes numbered upwards from 0 to the 4*Nk-1.

IV. EXISTING APPROACH

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.

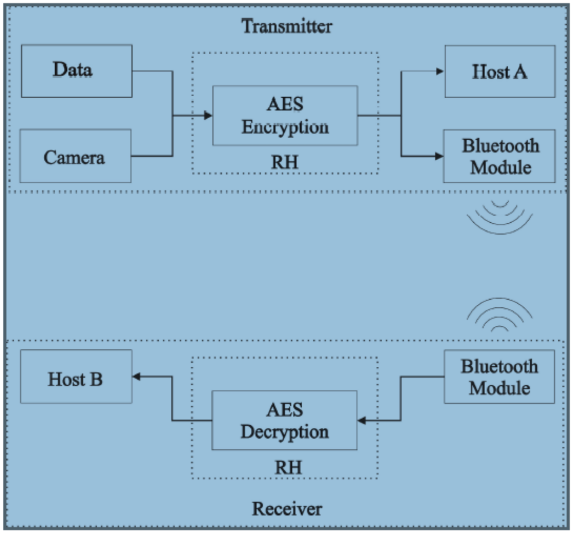

Fig 3: Existing Architecture.

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.

B. *Decryption*

The decryption process[7] 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.

V. PROPOSED APPROACH

This paper presents a compact implementation of advanced encryption standard

AES using different devices of FPGA technology. This implementation can be carried out through several trade-off between area and speed.

There are many techniques to design AES architecture to yield optimized implementation. Basic architecture in which each round manipulates 128 bit together and encrypts them by one clock cycle.

Pipelining in which throughput is increased versus area through adding more inner registers to achieve multiple processing simultaneously. Loop Unrolling in which k rounds are implemented rather than one round to gain high speed versus area. Chopping architecture in which the round data[3]width is decreased to one quarter of the basic round since the whole plain text needs looping four times to complete one round. This technique will gain compact area over speed. Proposed architecture is implementing 128 bits data-path for both cipher key and plaintext. The developed architecture combines basic architecture with one round and chopping technique to compromise the area with speed.

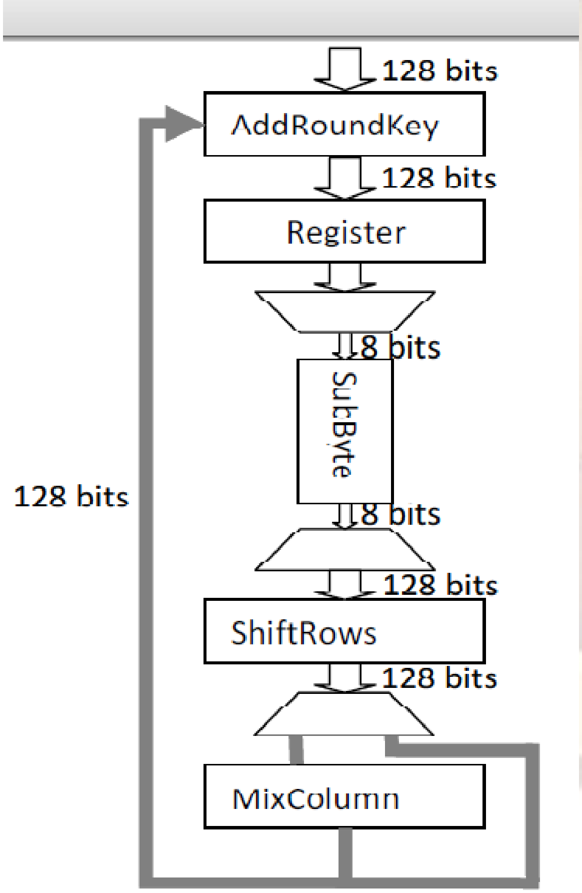

Fig 4: Proposed architecture.

Since the main point of the proposed architecture is to compromise the area and speed. Register-Transfer-Level (RTL) is checked frequently to avoid redundant hardware creation. Moreover, eliminate all in between registers and latches to save the use of RAM except at the beginning round.

VI. PERFORMANCE ANALYSIS

The proposed algorithm try to chopping the main block consuming the area “SBOX”, minimize in-between unwanted latches and shift registers to save area. Shift raw block is rejected and implemented by twisting the routing tracks. Mix column is implemented by combination gates. The proposed minimum area AES architecture[5]which is described by VHDL is simulated using ModelSim to verify the functionality as a primer verification tool. Moreover, the proposed algorithm is synthesized and implemented (translate, fit, place and route) using Xilinx 6.2. The proposed architecture is downloaded at FPGA kit is designed by the research team. Some blocks are added to communicate with Matlab program to check the algorithm since the plain text sent to FPGA and incoming cipher text is checked with the reference. Matlab file checks the comparison between reference pattern and incoming cipher text if they are matching an OK sign is printed otherwise false sign is printed.Not just a block by block is testing but a complete file of plaintext is used to check the algorithm to check its reliability. To be fair, the paper generates the keys and stores them to be used later in encryption so this comparison considers the stored keys algorithms not “on-the-fly” key schedule which affect deeply on the area consumption.

VII. CONCLUSION

This paper presents a compact implementation of advanced encryption standard AES using different devices of FPGA technology. This implementation can be carried out through several trade-off between area and speed. Compared to earlier techniques this paper proposes more efficient secure communication with network cryptographic techniques. The overall representation of these results gives high complexity with low cost and increasing network performance due to the presentation of the secure communication.

REFERENCES

[1] 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.

[2] K. J¨arvinen, M. Tommiska, and J. Skytt¨a. Comparative survey of high performance cryptographic algorithm implementations on FPGAs. In IEE Proceedings on Information Security, volume 152, pages 3 – 12, October 2005.

[3] Gaj, K and P. Chodowiec, “ Comparison of the hardware performance of the AES candidates using reconfigurable hardware”, Proceeding of RSA Security conference –

Cryptographer’s Track, San Francisco, CA,2001

[4] Ga¨el Rouvroy, Franc¸ois-Xavier Standaert, Jean-Jacques Quisquater and Jean-Didier Legat, “Compact and Efficient Encryption

[5] 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.

[6] Xinmiao Zhang and Keshab K. Parhi, “Implementation Approaches for the Advanced Encryption Standard Algorithm,” *IEEE Circuits and systems Magazine,* vol. 2, no. 4, pp. 24–46, 2003