International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.3, 2015

RESEARCH ARTICLE

ISSN: 2321-7758

FPGA IMPLEMENTATION OF SAFER+ ALGORITHM FOR BLUETOOTH SECURITY

M. ANANDRAJ[1], K. MURALIDHARAN[2], C. MEENAKSHI[3]

[1]Department of ECE, Anna university BIT campus, Tiruchirapalli
[2]Department of EEE, Coimbatore Institute of Technology, Coimbatore
[3]Department of EEE, Anna university Regional centre, Coimbatore

Article Received:07/05/2015 | Article Revised on:15/05/2015 | Article Accepted on:20/05/2015

M. ANANDRAJ

K. MURALIDHARAN

C. MEENAKSHI

ABSTRACT

The SAFER+ algorithm plays a major role in the authentication of Bluetooth mechanism. The data encryption and decryption of safer+ algorithm was done for 128 bit data with 128 bit key. The existing VLSI implementation of the SAFER+ algorithm uses the bit by bit modulo method for generating the key. In the proposed architecture the existing method is replaced and the parity bit generation method is used for key generation. A FPGA hardware kit was used for the hardware implementation of the algorithm. The proposed System implementation of the SAFER+ algorithm reduces the area coverage of about 25 percent, and 380 Mbps was achieved as a data throughput at a clock frequency of 20 MHz and proposed system achieves a high data throughput of about 760Mbits/sec at a maximum clock frequency of 44MHz, at reduced area cost . A comparative study was done between the algorithm properties and the VLSI architecture. The entire design of the algorithm was captured in VHDL language using a bottom-up design and verification methodology.

Key Words— Bluetooth, safer+ algorithm, cryptography

©KY Publications

I. INTRODUCTION

During the last years wireless communication technology has improved and having advanced devices now a days, Many new applications and opportunities were created. In addition, telecommunications devices and their supporting devices were fast growing . Special attention should be taken for connecting these devices effectively . Cable and infrared light are used for connecting the devices during the past years. Special connectors are needed and there are some complications in cable connectivity. This leads to malfunctions and major problems. The infrared light connectivity also have some problems such as line of sight and

distance. Because of these problems , Bluetooth technology [1],[2],have been established and developed for wireless communication. By using this communication system, wide range of computing and telecommunications devices were connected by the users simply. Wireless communications are easier and effective when compared to the cable connection. Bluetooth technology is now a days widely used in mobile phones Bluetooth uses the wireless LANs 802.11b technology, and this technology was designed for operating in low power over a short range, and data and voice services were supported. Peer-to-peer communications are established among many types of handheld devices and mobile . The major aim of this project is to execute the operation of implementation of the Safer+ algorithm [2]. The goal is to develop a safer+ algorithm and it achieves a high data throughput. SAFER+ algorithm belongs to the SAFER family of ciphers, and it contains the ciphers such as SAFER Key-64, SAFER Key-128, SAFER SecureKey-64, SAFER Secure Key- 128, and SAFER SecureKey-40. The block size of SAFER family may be 64 bits, 40 or 128 bits. The non-proprietary ciphers are used in the existing system[2]. James L. Massey developed at the ETH Zurich[4],[5],[6]. SAFER+ algorithm uses two types of ciphers .They are Feistel cipher and substitution-permutation cipher. The substitutions and permutations method are used for creating good confusion and diffusion instead of other methods. Byte-oriented block encryption algorithms are categorized with two properties. They are non-orthodox linear transformation, that is also known as Pseudo-Handmaid-Transformation (PHT) and the other one is additive constant factors (Bias vectors) and they are used in the scheduling for weak keys avoidance.

II. description of safer+ algorithm

The architecture of the SAFER+ algorithm [2] mainly comprised of two main components. They are the data encryption section and the key scheduling section. The plain text is passed for the r rounds of encryption and the r is calculated with the key length which is selected for the encryption. In this system the key size used for data encryption and decryption is 128 bits and the number of rounds needed for computation is eight. For each round of computation two 16-byte round sub keys are used .According to the user the round sub keys are determined based on the key scheduling.

The output comprises the encryption and the Xor/byte –addition operation is done for the"2 r-1" rounds. The cipher text of 16 -bytes is given as input for the safer+ decryption. The decryption only begins with the input trans-formation that only performs the output transform in the encryption process. The encryption process will be completed then the decryption process will start for r rounds of computation. The plain text is reproduced by the decryption process. The round sub keys are applied both for decryption and encryption .The keys are applied in the reverse order. The decryption structure [4] of SAFER + is shown in Fig.3. The input transformation is applied for the cipher text which is having identical r rounds transformation in the deciphering algorithm. The input transformation mainly contain the method of Mixed XOR/Byte-Subtraction of sub key K2r+1 is done in the input transformation of cipher text block. By reversing process the encrypted text is not converted into decrypted text because the encrypting rounds are different from decrypting rounds is the characteristic feature of safer+ algorithm. The output of input transformation is obtained with the 8-rounds of decryption. Required system throughput can be obtained with the minimized covered area in the modified single round implementation at same time the covered area is minimized. Data mapping and damping concepts are used in the modified architecture. Reverse function of the data mapping is done in the damping process .The proposed design will give the desired result in coverage area reduction than the existing system implementation. Mixed byte-addition/xor with a round key is added to the output of non-linear layer.

The four Pseudo-Handmaid-Transform (PHT) layer operations are performed and it is connected by three permutations. The decryption operation is the reverse operation for the encryption operation. The encryption and decryption structure are different structures . The keys are allocated in the reverse order in the decryption process. In the encryption process the keys are applied in normal order. SAFFER+ algorithm encryption [6] module is implemented as top level module. The other modules such as (sa-fer

single, modular addition, Bit wise ex-or, 'e' and 'l' blocks, permutation boxes, and Pseudo Handmaid Transform (PHT)) have been designed with top level module. The main block contains 128-bit key and 128-bit plain text is given as inputs and the received output will be 128-bit encrypted text.

A. Safer Encryption

SAFER+ algorithm encryption [6] module is implemented as top level module. The other modules such as (sa-fer single, modular addition, Bit wise operations like ex-or, 'e' and 'l' blocks, permutation boxes, and Pseudo Handmaid Transform (PHT)) have been designed with top level module. The main block contains 128-bit key and 128-bit plain text is given as inputs and the received output will be 128-bit encrypted text.

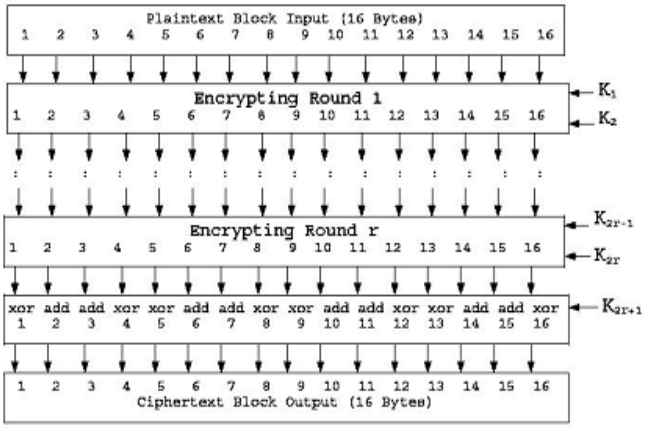

Fig.1. Encrypting structure

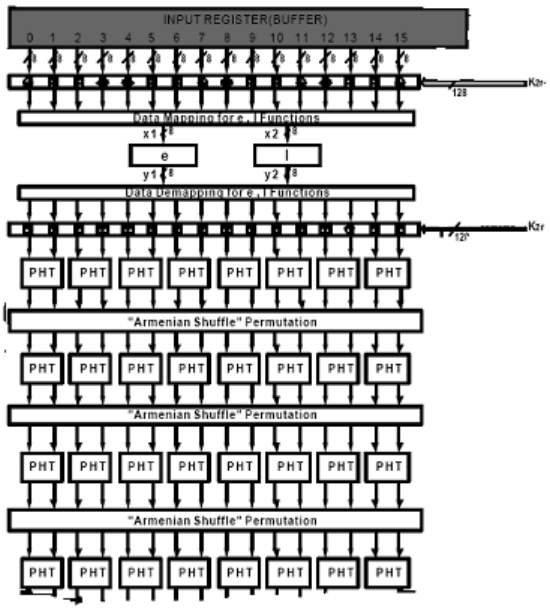

Fig.2.Modified Architecture

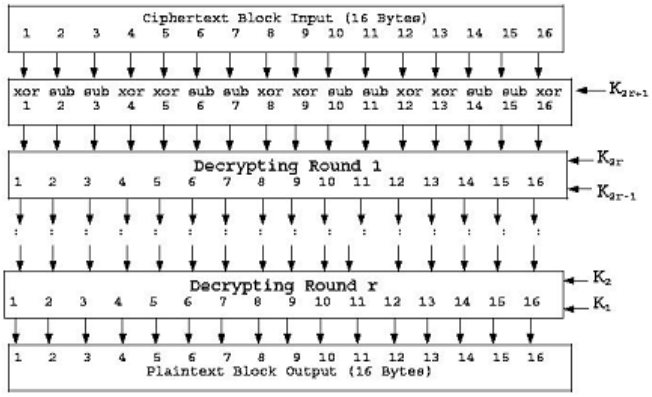

Fig.3.Decrypting Structure

B.Safer+ Decryption

In this implementation entire design was mainly divided in to Safer+ algorithm decryption and it is implemented as a top level module. The other modules such as (safer+ _desingle) modular subtraction, Bit wise ex-or, 'e' , 'l' blocks, inverse permutation boxes, and the reverse operation of Pseudo Handmaid Transform (IPHT)) that is inverse Pseudo hadamaid transform have been implemented as a top level module. The main block consider 128-bit key and 128-bit plain text was given as input and the output will be 128-bit cipher

III.SAFER+ SINGLE ROUND IMPLEMENTATION

In this proposed design the implementation single round SAFER+ algorithm is achieved. Eight loops of the single round implementation are required for running the whole safer+ algorithm. Required system throughput can be obtained and also the covered area will be minimized[6] in the single round implementation. This block will take two 128 bit keys and 128-bit plain text will be given as inputs and output will be 128-cipher.

A. Modular addition

Safer algorithm comprises four layers and 8-bit modular additions are performed in four layers. Interleaving of modular adders and bitwise ex-or takes place alternatively in every part of these four layers. Performance of modular addition is done over GF (256). In combination with modular addition blocks bit wise ex-or blocks are used in the safer+ single round implementation.

B.'E' and 'L' Blocks

Non-linearity is introduced in the substitution box layer of the safer+ algorithm and it is the

necessary feature of security. Substitution box comprises of non-linear functions such as 'e' ,'l' and they have been declared as follows:

e, l : {0, …, 255} → {0, …, 255} ,

e : I → (45i (mod 257))(mod 256) ,

l: I → j such that I = e(j) .

The eight 'e' and 'l' blocks are needed for the total algorithm. In the hardware implementation, one set of 'e' and 'l' blocks are used for minimizing the area.

The four linear PHT layers connected through the permutation PHT means Pseudo Handmaid Transform. The PHT boxes are declared as

PHT (in1, in2) = (2in1+ in2, in1+ in2).

The outputs of the PHT,

out1 = 2in1+ in2

out2 = in1+ in2

These are implemented in GF (256).

III.IPHT IMPLEMENTATION

IPHT stands for Inverse Pseudo Handmaid Transform. The IPHT boxes was declared as the outputs of the IPHT,

out1 = in1- in2

out2 = -in1+ 2in2

are implemented in GF (256).

Bit left wired shift was performed to achieve the Multiplication by 2 method in the IPHT block.

Four pht blocks and three blocks of permutations comprises of each single encryption round. Each pht block is having permutation. Changing byte positions which arise from pht block and it is performed by permutation block.

The permutation box performs the mapping of input bytes and output bytes and the permutation was done with input and output bytes. The 0 Position is mapped on 8 byte, 1 byte is mapped on 11 byte and the operations are performed by permutation box. In decryption process the re-verse operation of an encryption and the permutation was performed by the permutation box. Due to this reverse permutation and the decryption shows the same positions with the actual plaintext.

IV EXISTING SYSTEM

In the existing system the 128 bit text is given as input to the safer+ encryption and the key generation method used is bit by bit module method. The 128 bit key is used for both safer+ encryption and safer+ decryption.

VI PROBLEM STATEMENT

The major problem in the existing method is the bit by bit modulo method used in the key generation module. The data rate achieved with the FPGA device is slow with this method.

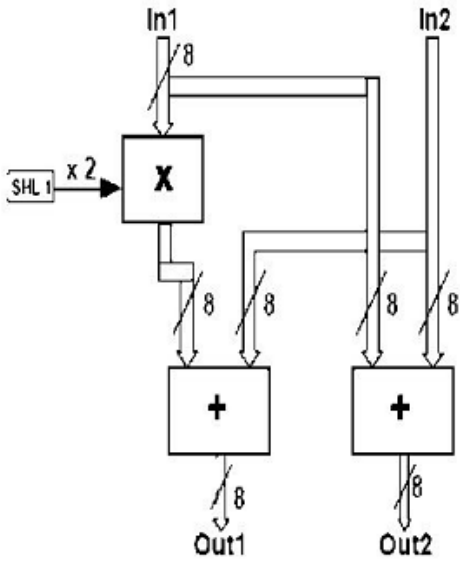

Fig.4.PHT Implementing Structure

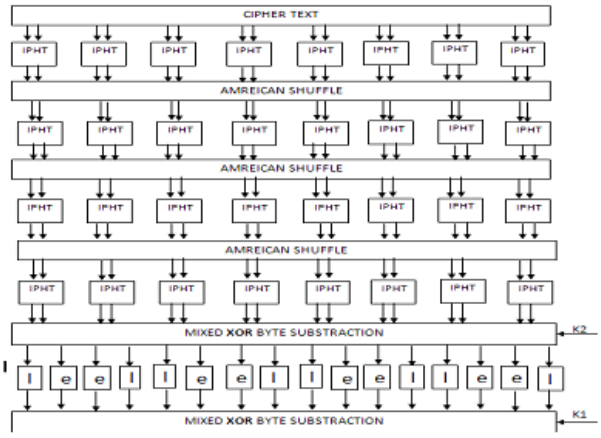

Fig.5.IPHT Structure

V PROPOSED SYSTEM

In the proposed system the key generation method is replaced with the parity bit key generation method. In order to improve the performance of the system and the throughput the key generation method is changed and the comparison results are shown.

VI SIMULATION RESULT AND DISCUSSION

The simulation was done for the Safer+ encryption and the plain text is given as input to the Safer+ encryption and the cipher text is received as output.

The simulation of Safer + decryption was done with the cipher text which is given as input to the Safer+ decryption block and the plain text is received as output.

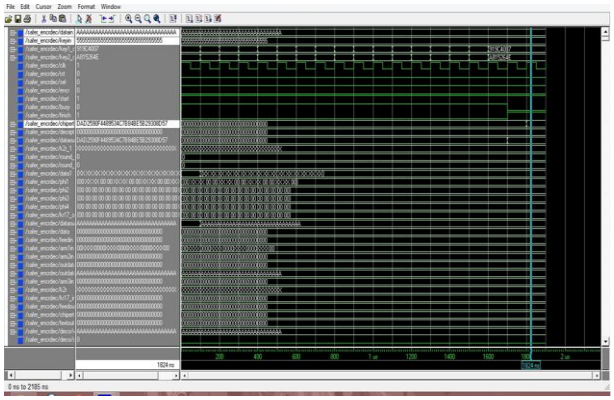

Fig.6.Simulated output of Encryption

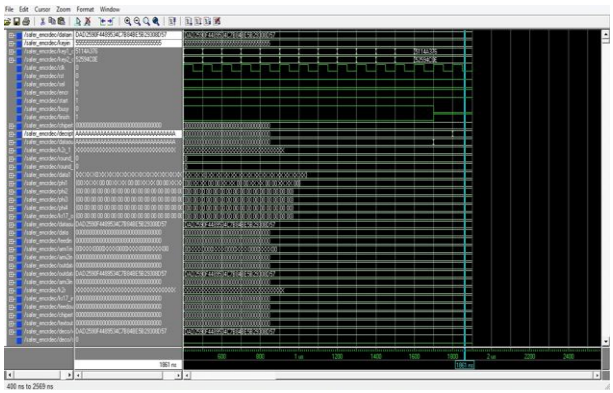

Fig.7.Simulated output of Decryption

The following table shows the result of frequency, Throughput and gate level count of the previous and proposed system.

Table:1 Comparative results of previous and proposed system

Type	Previous	Proposed
Gate level count required	233839	200002
Frequency	20	44
Throughput	380	760

VII CONCLUSION

In this paper, Safer+ algorithm implementation (which is most important algorithm) has been performed successfully with the help of FPGA. The complete knowledge of VHDL, simulation tools (Incisive (TM) unified si-mulator©5.6 and Modelsim © 6.0E) and some other synthesis tools(Encounter RTL Compiler-XL © Cadence Mentor Graphics © FPGA Advantage and Xilinx Web pack ISE 6.High throughput that is a datarate of 704Mbits/sec at a maxi-mum clock frequency of 44MHz has been achieved with the VLSI Implementation of SAFER + Algorithm. Comparisons between the proposed and previous implementations are delivered with the measured results.

VIII REFERENCES

[1] "Specification of the Bluetooth System", Specification Volume1, Version 1.1, February 22, 2001.

[2] J.L. Massey, G. H. Khachaturian, M. K. Kuregian, "Nomi-nation of SAFER+ as Candidate Algorithm for the Advance Encryption Standard", First Advanced Encryption

[3] Standard Candidate Conference, Ventura, CA, August 20-22, 1998.

[4] J. L. Massey, "On the Optimality of SAFER+ Diffusion",Second Advanced Encryption Standard Candidate Conference (AES2), Rome, Italy, March 22-23, on line available at http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm.

[5] J. L. Massey, "SAFER K-64: A Byte-Oriented Block Cipher-ing Algorithm", Fast Software Encryption, Proceedings of the

[6] Cambridge Security Workshop, Cambridge, U.K, 1998, pp. 1-17.

[7] P. Kitsos, N. Sklavos and O. Koufopavlou" HARDWARE IMPLEMENTATION OF THE SAFER ENCRYPTION ALGORITHM FOR THE BLUETOOTH SYSTEM" Vol. IV, pp. 878-881, USA, May 26-29, 2002

[8] Schubert, V. Meyer, W. Anheier, "Reusable Cryptographic VLSI Core Based on the SAFER K-128 Algorithm with 251,8 Mbits/s Throughtput", IEEE Workshop on Signal Processing Systems,1998,pp. 437-446

[9] Xilinx, San Jose, California, USA, Vertex, 2.5 V Field Programmable Gate Arrays, 2001, www.xilinx.com