Implementation of Data Encryption&Decryption For the Safer+ Algorithm Using Verilog HDL

J.Umesh rao, Dr.E.Nagabhooshanam

Abstract— A VLSI implementation for the SAFER+ encryption algorithm is presented. The combination of security and high speed implementation makes SAFER+ a very good choice for wireless systems. The SAFER+ algorithm is a basic component in the authentication Bluetooth mechanism. The relation between the algorithm properties and the VLSI architecture are described. The whole design was captured entirely in VHDL using a bottom-up design and verification methodology. A FPGA device was used for the hardware implementation of the algorithm. The proposed VLSI implementation of the SAFER+ algorithm reduces the covered area about 25 percent, and achieves a data throughput up to 320 Mbps at a clock frequency of 20 MHz and proposed architecture high data throughput of 704Mbits/sec at a maximum clock frequency of 44MHz, at a cost of area reduced.

Index Terms— Bluetooth Mechanishm, Cryptographic, Decryption, Encrypyion, Proposed Architecture, Safer+, Simulationresults.

1 INTRODUCTION

A Wireless communication technology has advanced at a very fast pace during the last years, creating new applications and opportunities. In addition, the number of computing and telecommunications devices is increasing. Special attention has to be given in order to connect efficiently these devices. In the past, cable and infrared light connectivity methods were used. The cable solution is complicated since it requires special connectors, cables and space. This produces a lot of malfunctions and connectivity problems. The infrared solution requires line of sight. In order to solve these problems a new technology, named Bluetooth [1], [2], has been developed. With this communication system, users are able to connect a wide range of computing and telecommunications devices easily and simply, without the need for connecting cables.Bluetooth is a technology and standard, designed as a wireless-cable replacement to connect a wide range of devices. Unlike wireless LANs such as 802.11b, it was designed to be low power, operate over a short range, and support both data and voice services. It enables peer-to-peer communications among many types of handheld and mobile devices. Furthermore, it provides a conceptually simple communication model and lets these devices exchange information and work together to benefit the user.The aim of this project is to develop a implementation of the Safer+ algorithm [2], The goal here is to develop a safer+ algorithm which achieves a high data throughput. The approach taken will be a prototype a mechanism in Verilog and simulate the same.

2 SAFER +

The SAFER+ (Secure and Fast Encryption Routine) algorithm is based on the existing SAFER family of ciphers, which comprises the ciphers SAFER K-64, SAFER K-128, SAFER SK-128 bits data[2].They have been developed by James L. Massey at the ETH Zurich[4],[5],[6]. SAFER+ (as is also the case with all prior ciphers in the SAFER family) is neither a Feistel cipher nor a substitution-permutation cipher.There is no fundamental reason to alternate between substitutions and permutations to create good confusion and diffusion.All algorithms are byte-oriented block encryption algorithms, which are characterized by the following two properties. First, they use a non-orthodox linear transformation, which, is called Pseudo-Handmaid-Transformation (PHT) for the desired diffusion, and second, they use additive constant factors (Bias vectors) in the scheduling for weak keys avoidance.

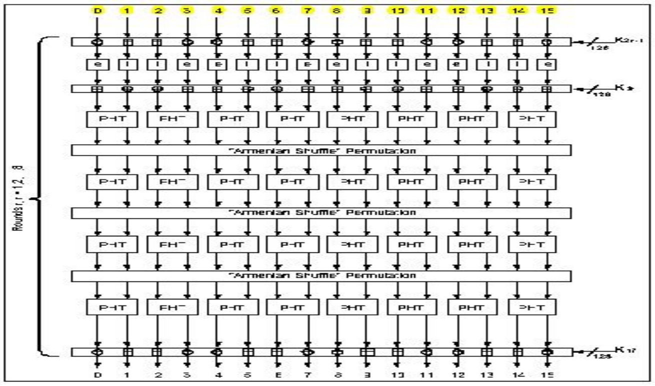


Fig. 1. One SAFER+ Encryption Round

2.1 Cryptographic Strength of Safer+

Differential cryptanalysis [2] has proved to be the most effec-

- *JARUPULA UMESH RAO received the B.Tech degree in ECEfrom VJIT, M.Tech in VLSI system design from Aurora scientific and technical research academy, Hyderabad.He is currently pursuing research in VLSI design from rayalaseema university, Kurnool.He has 7 years teaching experience, presently he is working as Associate professor in Nigama engineering college in the department of ECE.He is alife member of ISTE, he has published and presented 6 research papers in various reputed international/national journalas and conferances respectively. PH:+91-9676373876, E-mail: umesh481@gmail.com* tive general attack the previous SAFER family of ciphers, and appears also to be the most effective general attack against SAFER+.This task of showing the security of r-round SAFER+ against differential cryptanalysis is essentially that there are no (r-1)-round characteristics with probability greater than 2^{-128}.An exhaustive study of SAFER+ has shown that all 5-round characteristics have probability significantly smaller than 2^{-128}. The conclusion is that SAFER+ with six or more rounds is secure against differential cryptanalysis. SAFER+ enjoys good diffusion (i.e. to ensure that small changes in round inputs cause large changes in round outputs).also Ensures that "differences" similarly propagate and is the main source of the strength of SAFER+ against differential cryptanalysis.

3 ARCHITECTURE OF SAFER+ ALGORITHM

The architecture for the implementation of the SAFER+ algorithm [2] consists of the two main components, the data encryption path and the key scheduling. The plain text passes through the r rounds of encryption where r is determined by the key length chosen for the encryption. In our implementation we are using key size is 128 bits (fig.1), so the no of rounds becomes eight. Two 16-byte round sub keys are used within the each round of encryption. These round sub keys are determined from the user-selected key according to a key scheduling. Finally the last round sub key "2r+1" is to Mixed Xor/Byte –Addition with the r rounds of encryption. This addition constitutes the output transformation for safer+ encryption.The input for the decryption of the safer+ is the cipher text block of 16-bytes.The decryption begins with the input transformation that undoes the output transform in the encryption process. This block then process through the r rounds of decryption, round1 of which undoes the r round of encryption, round r undoes the encryption of round1 of encryption to produce the original plaintext. The round sub keys used for decryption used same as encryption but applied in reverse order.

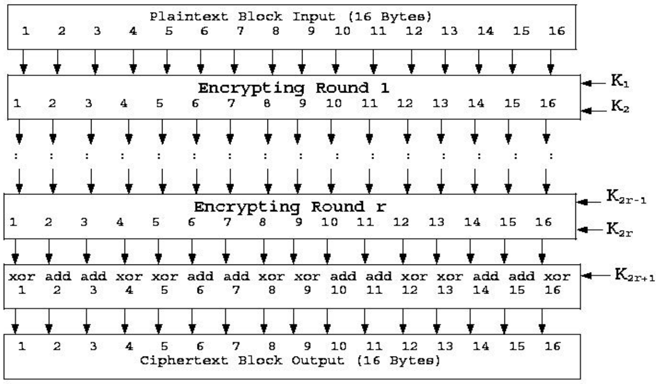

Plaintext Block Input (16 Bytes)
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Encrypting Round 1
K1
K2
Encrypting Round r
K2r-1
K2r
xor add add xor xor add add xor xor add add xor xor add add xor
K2r+1
Ciphertext Block Output (16 Bytes)

Fig. 2. The SAFER+ Encryption

3.1 Decryption of Safer+

The decrypting structure [4] of SAFER + is shown in Fig.3.The deciphering algorithm consists of an input transformation that is applied to the cipher text block, followed by r rounds of identical Transformations. The input transformation consists of the Mixed XOR/Byte-Subtraction of sub key K2r+1 from the cipher text block. A characterizing feature of SAFER+ is that decrypting rounds differ from encrypting rounds so that an encrypted cannot be converted to a decrypted by simply reversing the key schedule. The output of input transformation which undergoes the 8-rounds of decryption. The first round of decryption undoes the r round of encryption. The keys are used same as encryption but applied in reverse order.

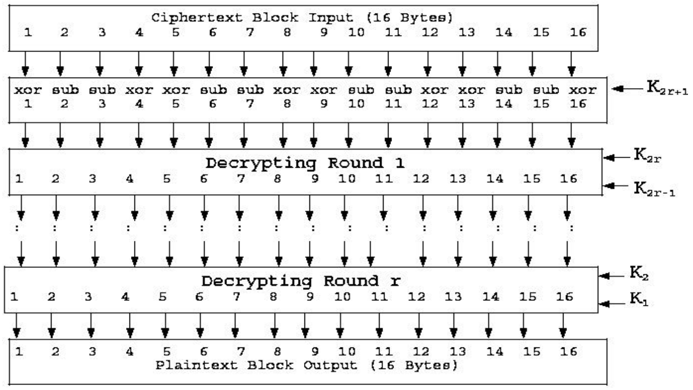

Ciphertext Block Input (16 Bytes)
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
xor sub sub xor xor sub sub xor xor sub sub xor xor sub sub xor
K2r+1
Decrypting Round 1
K2r
K2r-1
Decrypting Round r
K2
K1
Plaintext Block Output (16 Bytes)

Fig. 3. The SAFER+ Decryption

4 MODIFIED ARCHITECTURE

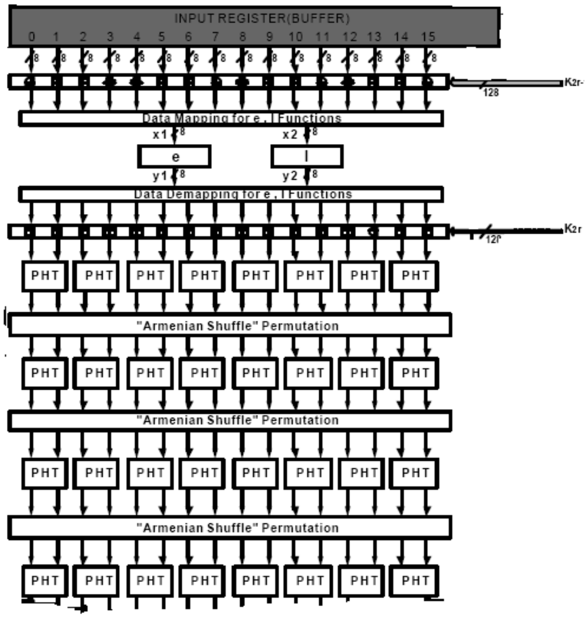

INPUT REGISTER(BUFFER)
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
8
K2r-
128
Data Mapping for e , l Functions
x1
x2
e
l
y1
y2
Data Demapping for e , l Functions
K2r
128
PHT
"Armenian Shuffle" Permutation

Fig. 4. Modified Architecture

The modified single round implementation is chosen because the required system throughput can be achieved and in the same time the covered area is minimized. In this modified architecture we use the concept of data mapping and damping. The damping unit performs the reverse function of the data mapping .This design results in reduction of the covered area than conventional implementations. After that the output of the nonlinear layer is added by a mixed byte-addition/xor with a round key.

The operations after that are four Pseudo-Handmaid-Transform (PHT) layer.That is connected through by three permutations. The decryption operation is reverse to the encryption operation. The encryption and decryption structure is dissimilar. In the decryption process the keys are applied in reverse order compared to the encryption process.

5 SAFER+ ENCRYPTION

In this implementation entire design has been divided in to various modules given below:

1. Safer encryption
2. Safer single
3. mod_add
4. xor_bit
5. e_block
6. l_block
7. permutation
8. pht

5.1 SAFER+ Encryption Implementation

SAFFER+ algorithm encryption [6].Implementation has been implemented as top level module. All other modules (safer single, modular addition, Bit wise ex-or, 'e' and 'l' blocks, permutation boxes, and Pseudo Handmaid Transform (PHT)) have been called in this top level module. The main block takes 128-bit key and 128-bit plain text as inputs and output will be 128-bit cipher.

5.2 SAFER+ single round implementation

In this proposed design the whole single round of the SAFER+ algorithm is implemented. In order to run the whole SAFER+ algorithm eight loops of the single round implementation are needed .The single round implementation[6] is chosen because the required system throughput can be achieved and in the same time the covered area is minimized. This block takes two 128 bit keys and 128-bit plain text as inputs and output will be 128-cipher.

5.3 Modular addition

Safer+ algorithm involves four layers of 8-bit modular additions. Modular adders and bitwise ex-or are interleaved alternatively in each of the four layers. This modular addition is performed over GF (256).

5.4 Bit EX-OR

Bit-wise ex-or blocks are also used in the single round of safer+ algorithm in combination with modular addition blocks.

5.5 'E' and 'L' Blocks

Substitution box layer introduces non-linearity to the safer+ algorithm which is an essential feature in any of the security algorithms. Substitution box contains 'e' and 'l' non-linear functions and have been defined as follows:

$$e, l : \{0, \ldots, 255\} \rightarrow \{0, \ldots, 255\} ,$$
$$e : i \rightarrow (45^i \pmod{257}) \pmod{256} ,$$
$$l: i \rightarrow j \text{ such that } i = e(j) .$$

In total eight 'e' and 'l' blocks are required for the algorithm. In the hardware implementation, to minimize the area only one set of 'e' and 'l' blocks are used

5.6 PHT Round

The four linear PHT layers connected through the permutations as shown in Figure.5

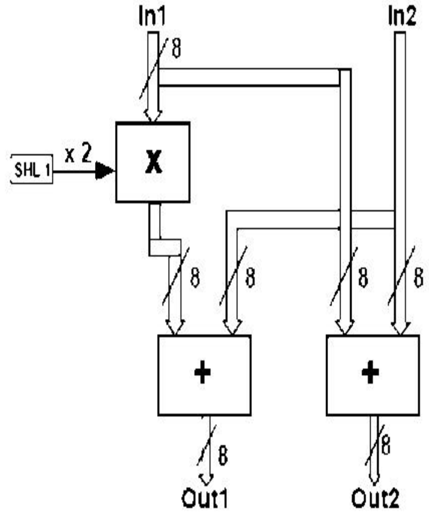


Fig. 5. Permutation boxes

PHT stands for Pseudo Handmaid Transform. The PHT boxes defined as

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

The outputs of the PHT,

out1 = 2in1+ in2

out2 = in1+ in2 are implemented in GF (256).

6 SAFER+ DECRYPTION

In this implementation entire design has been divided in to various modules given below.

1. Safer decryption
2. Safer_desingle
3. Mod_subtract
4. Inverse permutation
5. Inverse pht

6.1 SAFER+ Decryption Implementation

Safer+ algorithm decryption implementation has been implemented as top level module. All other modules (safer+_desingle) modular subtraction, Bit wise ex-or, 'e' and 'l' blocks, inverse permutation boxes, and inverse Pseudo Handmaid Transform (IPHT)) have been called in this top level module. The main block takes 128-bit key and 128-bit plain text as inputs and output will be 128-bit cipher.

6.2 IPHT Block

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

out1 = in1- in2

out2 = -in1+ 2in2 are implemented in GF (256).

Single IPHT block implementation is shown in Figure 3.9.In IPHT block Multiplication by 2 can be achieved by one bit left wired shift.

In the each single round of an encryption consists of a four pht blocks and three blocks of permutations. Permutation is after the each pht block. The permutation block performs the change the byte positions which are came from pht block.

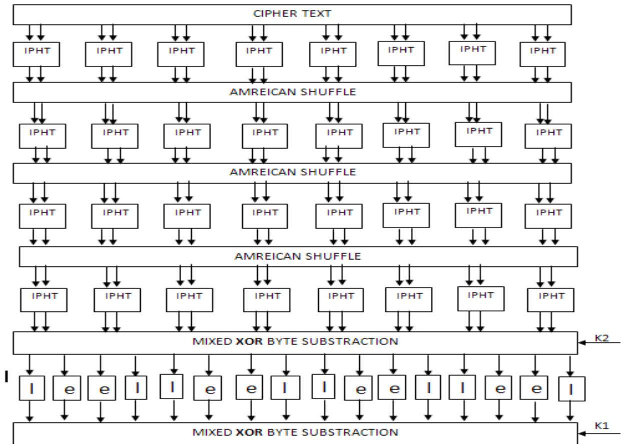

CIPHER TEXT
IPHT
AMREICAN SHUFFLE
IPHT
AMREICAN SHUFFLE
IPHT
AMREICAN SHUFFLE
IPHT
MIXED XOR BYTE SUBSTRACTION
K2
I
l e e l l e e l l e e l l e e l
MIXED XOR BYTE SUBSTRACTION
K1

Fig. 6. The IPHT Implementation

The permutation box performs the how the input bytes are indices are mapped into output bytes. Thus Position 0(left most) is mapped on 8 byte; byte 1 is mapped on 11 byte like that the permutation box performs the operation. In the process of decryption the permutation box performs the reverse the operation of an encryption permutation. Due to this reverse permutation in decryption causes the same positions in actual plaintext.

7 VERILOG HDL

Implementation of High Speed CRC is done using Verilog HDL.In the semiconductor and electronic design industry, Verilog is a hardware description language (HDL) used to model electronic systems. Verilog HDL, not to be confused with VHDL, is most commonly used in the design, verification, and implementation of digital logic chips at the Register transfer level (RTL) level of abstraction. It is also used in the verification of analog and mixed-signal circuits.

7.1 Experimental and Simulation Results

The whole design was captured entirely in verilog HDL language. All of the system components have been described with structural architecture.The proposed architecture is synthesized by using FPGA device of XILINX [7].

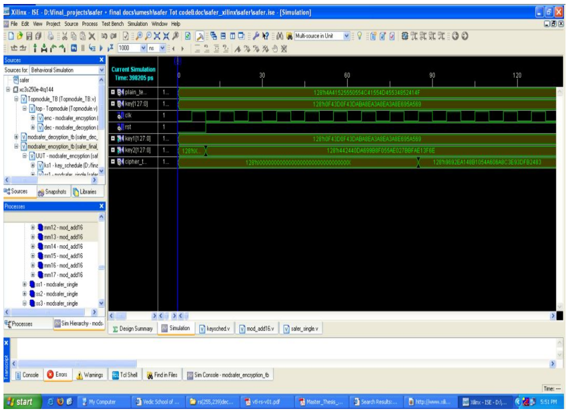
Final Timing Optimization Statistics for the design

• Clk	: 44 MHz
• FPGA used for synthesis	: VIRTEX IV-PRO
• Devices used	: 12ff152
• Throughput	: 704Mbits/sec

TABLE 1

COMPARISION BETWEEN PREVIOUS AND MODIFIED ARCHITECTURE

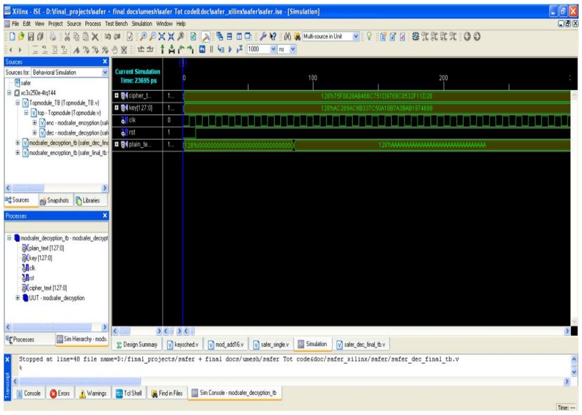
Type	Previous	Proposed
Gate level count required	233839	200013
Frequency	20 MHz	44 MHz
Throughput	320Mbits/sec	704Mbits/sec


Xilinx - ISE - D:\final_projects\safer + final docs\umesh\safer Tot code&doc\safer_xilinx\safer\safer.ise - [Simulation]

Current Simulation Time: 398205 ps

plain_te...	1...	128'h4A41525550554C41554D4553485241 4F
key[127:0]	1...	128'h0F43D0F43DABA8EA3A8EA3A8E695A569
clk	1	
rst	1	
key1[127:0]	1...	128'h0F43D0F43DABA8EA3A8EA3A8E695A569
key2[127:0]	1...	128'hX... 128'h442440DA699B8F055AE027BBFAE13F6E
cipher_t...	1...	128'hXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX 128'h9692EA148B1054A606A8C3E93DFB2483

Fig. 7. Simulation results of Safer+ encryption


Xilinx - ISE - D:\final_projects\safer + final docs\umesh\safer Tot code&doc\safer_xilinx\safer\safer.ise - [Simulation]

Current Simulation Time: 23695 ps

cipher_t...	1...	128'h75F0828AB466C751D9769C0532F11D28
key[127:0]	1...	128'hAC285AC9B337C50A10B7A3BAB1974688
clk	0	
rst	1	
plain_te...	1...	128'hXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX 128'hAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

```
Stopped at line=48 file name=D:/final_projects/safer + final docs/umesh/safer Tot code&doc/safer_xilinx/safer/safer_dec_final_tb.v
%
```

Fig. 8. Simulation results of Safer+ decryption

8 CONCLUSION

In this project, implementation of Safer+ algorithm (which is most important algorithm) has been carried out successfully has been done. This project has helped me to become familiar with Verilog HDL, simulation tools (Incisive (TM) unified simulator©5.6 and Modelsim© 6.0E) and various synthesis tools (Encounter RTL Compiler-XL©Cadence Mentor Graphics© FPGA Advantage and Xilinx Web pack ISE 6.1i). FPGA device has been used for the implementation of the algorithm. VLSI implementation of the SAFER+ algorithm has been observed to work with a high throughput of 704Mbits/sec at a maximum clock frequency of 44MHz, at a cost of area reduced. Measurement results and comparisons between the proposed and previous implementations are presented.

ACKNOWLEDGEMENT

The author would like to acknowledge the support of the author's supervisor, professor and head Dr.E. Nagabhooshnam (MGIT) and Mr.S.Ramesh babu (NEC) for their continuous interest, encouragement and guidance through out the research. This research is supported by Rayalaseema univer sity, Kurnool and Nigama engineering college, karim ngar.The author would also like to thank everybody who was involved directly or indirectly in the research project, especially the author would like to express his heartful thanks for the support given by the secretry and joint secretry of NEC, karimnagar.

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, "Nomination of SAFER+ as Candidate Algorithm for the Advance Encryption Standard", *First Advanced Encryption Standard Candidate Conference,* Ventura, CA, August 20-22, 1998.

[3] 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.

[4] J. L. Massey, "SAFER K-64: A Byte-Oriented Block Ciphering Algorithm", *Fast Software Encryption,* Proceedings of the Cambridge Security Workshop, Cambridge, U.K, 1998, pp. 1-17.

[5] 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

[6] A. 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

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