A VLSI IMPLEMENTATION OF A RESOURCE EFFICIENT AND SECURE ARCHITECTURE OF A BLOCK CIPHER

Satish Shivaram[1], R.Krishna[2], Vijayaprakash[3], K.V.Prasad[4]

[1]*Student, Electronics and Communication, Bangalore Institute of Technology, Karnataka, India.*
[2]*Assistant Professor, Electronics and communication, Bangalore Institute of Technology, Karnataka, India.*
[3]*Professor, Electronics and Communication, Bangalore Institute of Technology, Karnataka , India.*
[4]*Professor and HOD, Electronics and Communication, Bangalore Institute of Technology, Karnataka, India.*

Abstract

In today‘s modern life, the protection of data is of major concern in any kind of domian. So the understanding of cryptography architecture plays a crucial role. Advance encryption system , differential encryption system design of cryptography have few drawbacks in implementation level of low level designs. In an area concerned and power concerned parameters the above mentioned algorithms have failed in implementing. The humming bird algorithm uses block cipher which is being used in this paper for encryption and decryption using 128 bit secure key. Block cipher concentrates on converting the given original data into cipher text to make the given data more secure over the user. Two different designs of block Cipher algorithms (Throughput enhanced , Area reduced) are developed and their performance is compared in terms of area occupation using Xilinx ISE design tool with verilog language. The block cipher designs are implemented using 64 bit secure key and 128 bit secure key. The area reduced design is of the concern to have this module on the FPGA implementation in the VLSI sector.

***Keywords :** Cryptography, VLSI, FPGA , Block Cipher.*

--***--

1. INTRODUCTION

After the computer invention the need of developing tools to protect the information (data) stored in the computer raised. To fulfill this requirements number of tools designed and developed with the main goal of protecting information present in the computer from hackers. These facilities are generally called as computer security. The development of communication and network facilities make it possible to share the information between computers and then the problem of hacking of information arises from this the concept of network security developed.

Cryptography is a technique that makes information not readable by unauthorized persons, by the use of encoding method. Some of the application of cryptography includes the security of ATM cards, use of passwords in computer and electronic commerce. Cryptography is derived from the Greek words ‗kryptos‘(hidden) and ‗graphos‘(written) respectively. Cryptography involves two processes. These are encryption and decryption. Encryption converts the plain text to cipher text. Decryption converts cipher text to plain text.

The main goal of cryptography is to make our information confidential. There are various cryptographic algorithms have been developed. The design of any cryptographic algorithm requires the focus on three parameter: these are ―security, cost and performance‖. So depending on particular application one can choose better algorithm suitable for that application.

Standardized algorithms like AES, DES etc, fails to provide security in applications such as RFID tag, sensor nodes, and smart cards. These algorithms demands the support of more resources, lightweight cryptography can be used as an alternative for these application, which gives better security compared to standardized cryptographic algorithms. This gives motivation for the designer to move towards lightweight cryptographic algorithms.

Hummingbird cryptography is one of the lightweight cryptographic algorithms. Design of Hummingbird cryptography is motivated by the enigma machine . It is found that it uses small sized block and able to withstand cryptographic attacks like linear and differential cryptanalysis.

In this paper hummingbird cryptographic algorithm is considered and tries to modify the block cipher used to reduce the area and enhanced performance without affecting the security of algorithm.

In this paper block cipher is designed using throughput enhanced and area reduced architecture. The secure key used in this paper is 128 bit instead of 64 bit which was used in previous work. The S-box used here makes use of the readily available LUT which is shown in the methodology section. Both encryption and decryption work are carried out to show the given plain text is secured in high terms with large number of bits. With the same key used the given plain text can be obtained making the information more secure. The area utilization of both throughput enhanced and area reduced are obtained by synthesis report by using Xilinx 14.6 and are compared. Simulation results are obtained using ModelSim 10.1 and the waveforms are observed.

The Theoretical backgrounds of cipher block and proposed architecture will be described in the next two sections. The simulation results and synthesis report will be discussed before conclusion.

2. THEORETICAL BACKGROUND

In this section the basic flow chart of through put enhanced design and area reduced design is incorporated.

In the first step the 16 bit plain text data is mixed with the 128 bit secure key which is subdivided into 8 different 16 bit secure key. Followed by this step is substitution step where the S-box plays an important role for both encryption and decryption. In this paper readily available S-box LUT is being used instead of representing Boolean expressions. linear transformation is followed after substitution layer. After eight times iteration the second round key with exoring with all odd numbers of key is given to S-box and linear transform layer. The process is repeated as shown in fig 1.

The readily available S-box is shown below.

Table 1: S-Boxes given in Hexadecimal format

x	0	1	2	3	4	5	6	7
$S_1(x)$	8	6	5	F	1	C	A	9
$S_2(x)$	0	7	E	1	5	B	8	2
$S_3(x)$	2	E	F	5	C	1	9	A
$S_4(x)$	0	7	3	4	C	1	A	F
x	8	9	A	B	C	D	E	F
$S_1(x)$	E	B	2	4	7	0	D	3
$S_2(x)$	3	A	D	6	F	C	4	9
$S_3(x)$	B	4	6	8	0	7	3	D
$S_4(x)$	D	E	6	B	2	8	9	5

3. PROPOSED ARCHITECTURE

a. Throughput enhanced design:

In this paper, the cipher block is presented by new expressions. The encryption and decryption block is designed separately using 128 bit has the new proposed design. The basic design of throughput enhanced design of block cipher using 128 bit secure key is as shown in fig 1.

The proposed work goes well with the theoretical background with flow chart starting with the key mixing step with the given plain text. Followed by substitution layer where S- box plays an important role. In this paper we are using readily available S-box as shown in table 1.

Followed by linear transformation layer which is given by m^m<<6^m<<10 expression for encryption. These steps are repeated 8 times with different 16 bit secure key.

K9 is calculated with all the odd numbers of keys exoring and leads to S-box substitution and linear transformation and then k10 is calculated with all the even number of keys. The final 16 bit encrypted data of the given plain text data is obtained which is further made use in the decryption block using the same 128 bit secure key.

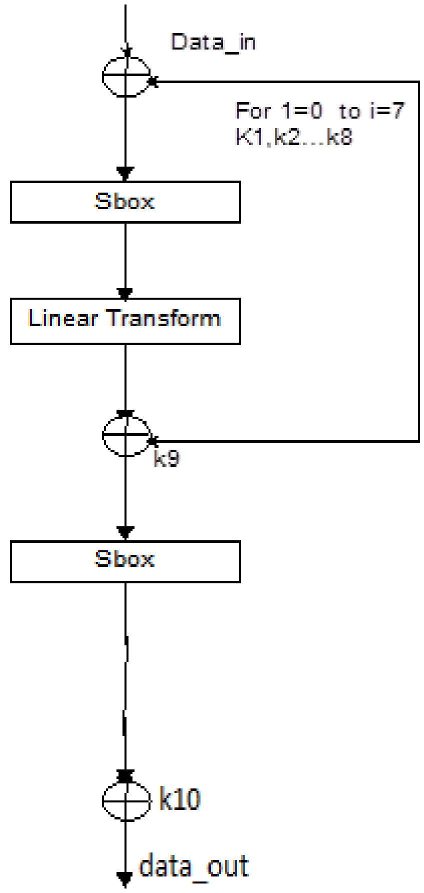


Fig 1. Block diagram of proposed throughput enhanced encryption unit

The decryption block using 128 bit secure key is as shown in fig 2. Here the operation are carried out in a similar manner as compared to encryption block which is the mirror operation of it.

The only difference is the way the S-box readings are made which is inverse. In the next inverse linear transform the expression is given by m^m<<6^m<<10^m<<12. All the operations are inversed starting from key k10 to k1. The decrypted data is same as the plain text given and the procedure followed serves the purpose.

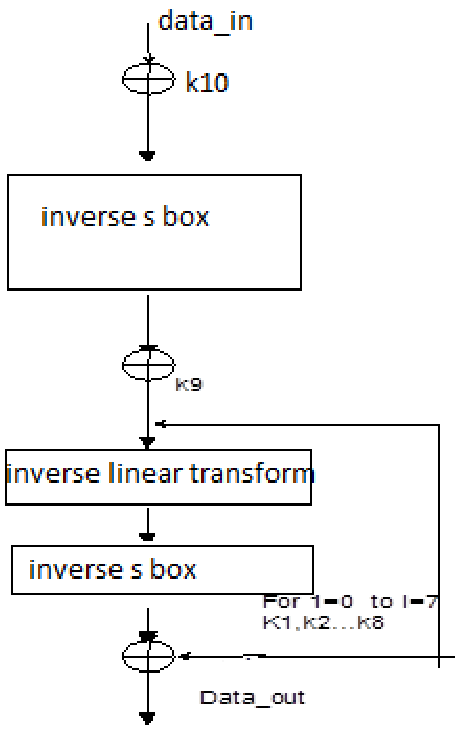


Fig 2. Block diagram of proposed throughput enhanced decryption unit.

b. area reduced design:

in this paper major proposal is to get area reduction on fpga. The area reduced design encryption is shown in fig 3.

In this design the number of components are reduced in the first part of substitution and linear transformation unit. The eight iterations are reduced with one unit where each key processing output is stored in a flop and based on the key select and data select operations are performed and the synthesis report is been generated and compared with the throughput enhanced version. We can see the number of 4 input LUTs used is reduced in this design.

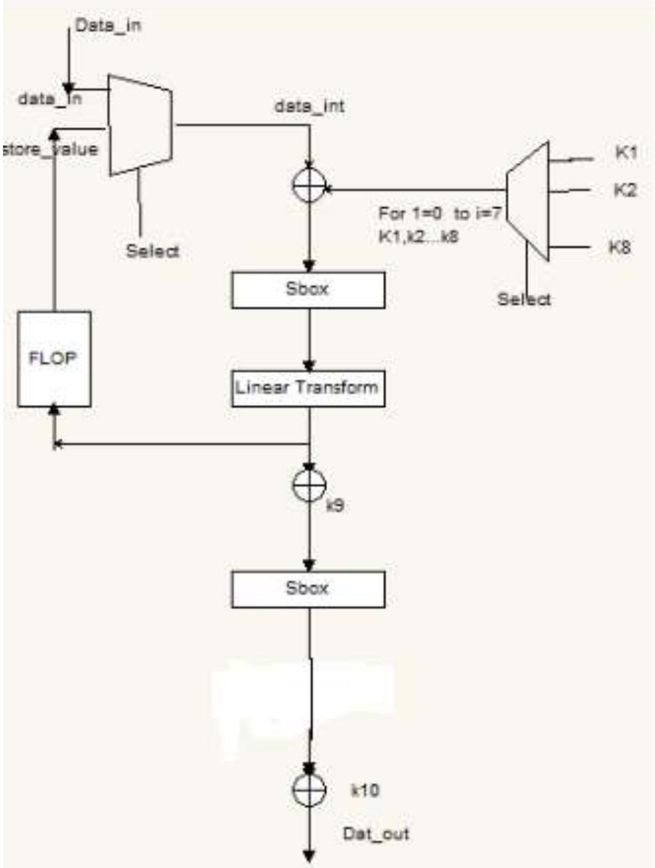
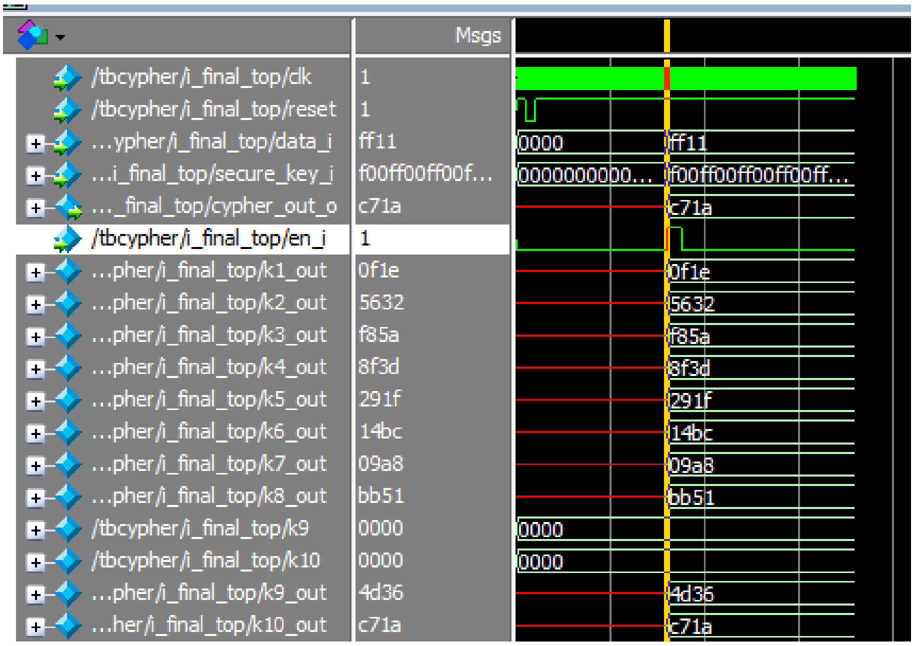


Fig 3. Block diagram of proposed area reduced design unit.

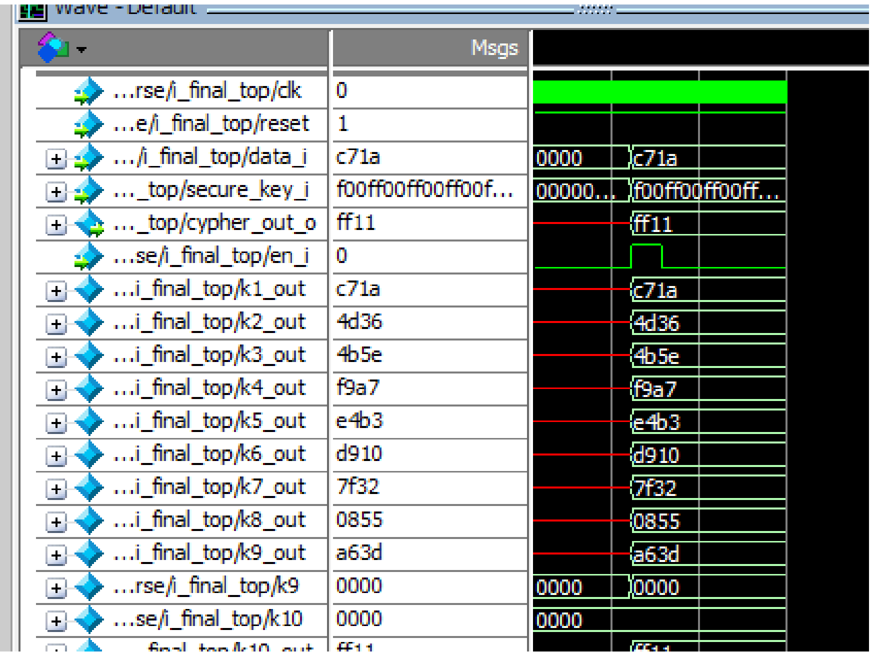
Simulation results:

Simulation results are seen using ModelSim 10.1b



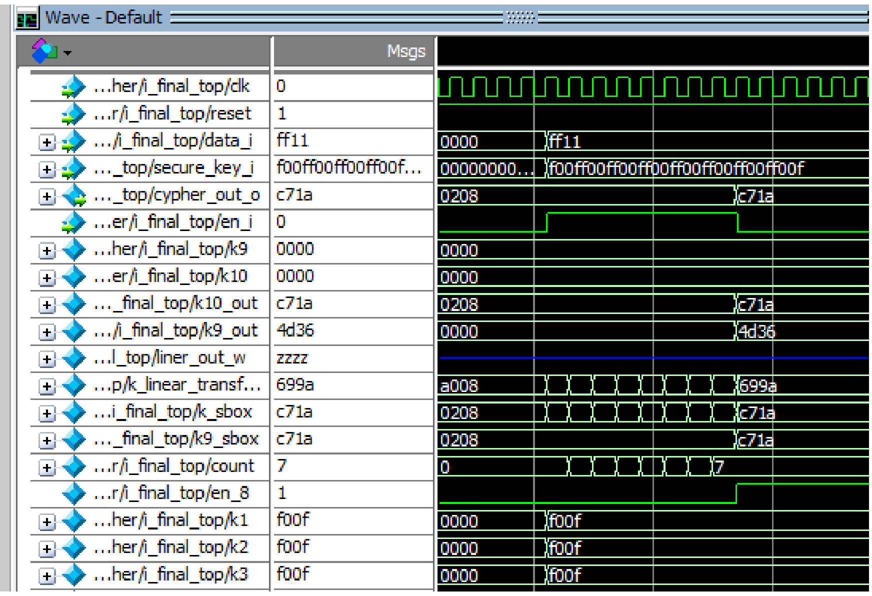
	Msgs
/tbcypher/i_final_top/clk	1
/tbcypher/i_final_top/reset	1
...ypher/i_final_top/data_i	ff11
...i_final_top/secure_key_i	f00ff00ff00f...
..._final_top/cypher_out_o	c71a
/tbcypher/i_final_top/en_i	1
...pher/i_final_top/k1_out	0f1e
...pher/i_final_top/k2_out	5632
...pher/i_final_top/k3_out	f85a
...pher/i_final_top/k4_out	8f3d
...pher/i_final_top/k5_out	291f
...pher/i_final_top/k6_out	14bc
...pher/i_final_top/k7_out	09a8
...pher/i_final_top/k8_out	bb51
/tbcypher/i_final_top/k9	0000
/tbcypher/i_final_top/k10	0000
...pher/i_final_top/k9_out	4d36
...her/i_final_top/k10_out	c71a

Fig 4. Waveform of throughput enhanced encryption using 128 bit secure key.



```
Wave - Default
                         Msgs
…rse/i_final_top/clk     0
…e/i_final_top/reset     1
…/i_final_top/data_i     c71a
…_top/secure_key_i       f00ff00ff00ff00f…
…_top/cypher_out_o       ff11
…se/i_final_top/en_i     0
…i_final_top/k1_out      c71a
…i_final_top/k2_out      4d36
…i_final_top/k3_out      4b5e
…i_final_top/k4_out      f9a7
…i_final_top/k5_out      e4b3
…i_final_top/k6_out      d910
…i_final_top/k7_out      7f32
…i_final_top/k8_out      0855
…i_final_top/k9_out      a63d
…rse/i_final_top/k9      0000
…se/i_final_top/k10      0000
```

Fig 5. waveform of throughput enhanced decryption unit using 128 bit secure key



```
Wave - Default
                         Msgs
…her/i_final_top/clk     0
…r/i_final_top/reset     1
…/i_final_top/data_i     ff11
…_top/secure_key_i       f00ff00ff00ff00f…
…_top/cypher_out_o       c71a
…er/i_final_top/en_i     0
…her/i_final_top/k9      0000
…er/i_final_top/k10      0000
…_final_top/k10_out      c71a
…/i_final_top/k9_out     4d36
…l_top/liner_out_w       zzzz
…p/k_linear_transf…      699a
…i_final_top/k_sbox      c71a
…_final_top/k9_sbox      c71a
…r/i_final_top/count     7
…r/i_final_top/en_8      1
…her/i_final_top/k1      f00f
…her/i_final_top/k2      f00f
…her/i_final_top/k3      f00f
```

Fig 6. waveform of area reduced encryption unit using 128 bit secure key.Synthesis report :

Syntesis is done using Xilinx 14.6 version.

Table 2: Device utilization summary

Module	Area in LUT
Throughput Oriented 128	252
Area oriented 128	104
Through put base paper 64	132
Area oriented 64	88

CONCLUSION

In this paper , the cipher block named throughput enhanced and area reduced block ciphers are implemented. Both encryption and decryption units are developed and implemented. The round keys are generated and registered using 128 bit secure key instead of 64 bit key used in the previous work. The S – box implementation is done using readily available LUTs instead of Boolean expression which is time consuming and more number of slices for implementation.

The simulation and synthesis reports are tabulated . as seen from the table 2 area reduced design required lesser number of 4 input LUT compared to throughput enhanced design. This shows that single module chip area optimization is observed in greater manner. This is a well balanced architecture with high performance and low complexity. This cipher block can also be used in wireless sensor nodes and smart chips.

REFERENCES

[1] R. Anderson, E. Biham, and L. Knudsen, "Serpent: A proposal for the advanced encryption standard," in *Proc. 1st Advanced Encryption Standard (AES) Conf.*, 1998.

[2] B. Singh, L. Alexander, and S. Burman, "On algebraic relations of Serpent S-boxes", Cryptology ePrint Archive, Report 2009/038, 2009.

[3] M. J. O. Saarinen, "Cryptanalysis of Hummingbird-1," in *Proc. the 18th international conference on Fast software encryption*, Denmark, Feb. 2011.

[4] C. Patterson, "A Dynamic FPGA Implementation of the Serpent Block Cipher," *Lecture Notes in Computer Science*, Vol. 1965, pp 141-155, 2000.

[5] X. Fan, H. Hu, G. Gong, E. Smith, and D. Engels, "Lightweight Implementation of Hummingbird Cryptographic Algorithm on 4-Bit Microcontrollers," in *Proc. 4th International Conference for Internet Technology and Secured Transactions (ICITST 2009)*, pp. 838-844, Nov. 2009.

[6] X. Fan, G. Gong, K. Lauffenburger, and T. Hicks, "FPGA Implementations of the Hummingbird Cryptographic Algorithm," in *Proc. The 2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST 2010)*, pp.48-51, 2010.

[7] X. Chen, Y. Zhu, Z. Gong, and Y. Luo, "Cryptanalysis of the Lightweight Block Cipher Hummingbird-1," in *proc. Fourth International Conference on Emerging Intelligent Data and Web Technologies (EIDWT)*, pp. 515 - 518, 2013.

[8] I. San and N. At, "Compact Hardware Architecture for Hummingbird Cryptographic Algorithm," in *Proc. 2011 International Conference on Field Programmable Logic and Applications (FPL)*, pp.376-381, Sept. 2011.

[9] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher", *Cryptographic Hardware and Embedded Systems*, vol. 4727,Springer Heidelber, pp. 450-466, 2007.

[10] G. Xianwei,L. Erhong, X. Liqin, C. Hanlin, "FPGA Implementation of the SMS4 Block Cipher in the Chinese WAPI Standard," in *Proc. International Conference on Embedded Software and Systems Symposia*, pp.104-106, July 2008.

[11] X. Fan, "Efficient Cryptographic Algorithms and Protocols for Mobile Ad Hoc Networks," Ph.D. thesis, University of Waterloo, Canada, March 2010.

[12] P. Bora and T. Czajka,"Implementation of the Serpent Algorithm Using Altera FPGA Devices," Public Comments on AES Candidate Algorithms-Round 2, available at : http://www.nist.gov/aes/.

[13] A.J. Elbirt and C Paar, "An FPGA implementation and performance evaluation of the Serpent block cipher," In *Proc. ACM Eighth International Symposium on Field Programmable Gate Arrays (FPGA 2000)*, pp. 33–40, Feb 2000.

[14] X. Fan, G. Gong, and H. Hu, "Remedying the Hummingbird Cryptographic Algorithm," in *Proc. The 2011 IEEE International Workshop on Security and Privacy in Internet of Things (SPIoT 2011)*, China, Nov. 2011.

[15]Saha, Shumit, Md. Rashedul Islam, Habibur Rahman, Mehadi Hassan, and A. B. M. Aowlad Hossain. "Design and implementation of block cipher in hummingbird algorithm over FPGA", Fifth International Conference on Computing Communications and Networking Technologies (ICCCNT), 2014.