11th International Conference on Recent Trends in Engineering, Science and Management
(IETE) Institution of Electronics and Telecommunication Engineers, Osmania University Campus, Hyderabad, India
22nd October 2017, www.conferenceworld.in (ICRTESM-17) ISBN: 978-93-86171-72-6

Design and Implementation of Three Fish Cipher Algorithm Blocks Using FPGA

V. Vijaya[1], Ramavath.Anusuria[2], N. Surya[3],

[1]*M. Tech, SRIET, Hyderabad, Telangana (India)*

[2,3]*Asst. Professor, TKRCET, Hyderabad, Telangana (India)*

ABSTRACT

Every organization sees the secure communication is the prime requirement. In today's world the security has became the major aspect of life. It can be achieved by various techniques such as password, cryptography and biometrics. In this work, to study various encryption algorithms, data encryption standard used for data security and implement Three-Fish Cipher algorithm in order to achieve security with minimum number of overheads then compare the proposed work with test bench and then compile, simulate the test bench with the help of Xilinx ISE software.

***Key Index:* Secure communication, Three-Fish Cipher algorithm, Xilinx ISE software.**

I. INTRODUCTION

Data Encryption Standard (DES) is the most well-known cryptographic mechanism in history [1]. It begins with the work of Feistel at IBM in the early 1970s. Ruth M. Davis [3] provides a hardware-implementable algorithm for enciphering data, which has been adopted as a Federal standard to provide a high level of cryptographic protection against various attacks. Whitfleld Diffie et. al [4] describes cryptographic technology, which examines the forces driving public development of cryptography. Ingrid Verbauwhede [5] described Security and Performance Optimization of a New DES Data Encryption Chip. James E. Katz [6] provides Social Aspects of Telecommunications Security Policy for privacy and of society for security. H. Bonnenbergt [7] described the VLSI implementation of a new block cipher. K.H. Mundt [8] presented superscript ASIC get 100Mbits/ s encryption speed on silicon applying 1 micron design rules. C. Boyd [9] provides the modern data encryption in which proposed standard for digital signatures based on RSA were introduced. R. Zimmermann et. al. [10] provides a 177 Mb/s VLSI implementation of the International Data Encryption Algorithm. Stefan Wolter [11] provides the implementation of the IDEA architecture that includes a concurrent self-test based on a mod3 residue code self-checking system. Seung-Jo Han [12] describes the improved DES algorithm in which a 96-bit data block is divided into three 32-bit sub-blocks. Hassina Guendouz et. al. [13] describes rapid prototype of a fast data encryption standard with integrity processing for cryptographic applications. K. Wong [14] performed transform domain analysis of DES algorithm by using tool. M.P. Leong [15] described a bit-serial implementation of the International Data Encryption Algorithm (IDEA). R. G. Sixel et. al. [16] describes a high level language implementation of the DES and bit-slice architecture. Teo Pock Chueng [17] provides implementation of pipelined DES using Alter CPLD. Toby Schaffer et. al. [19] describes an integrated design of

Advanced Encryption Standard (AES). Cameron Patterson [20] provides high performance DES encryption using Vertex FPGA. Jbits. Pui-Lam Siu et. al. [22] presented about the A Fault Attack on pairing based Cryptography Current fault attacks against public key cryptography focus on traditional schemes.

II. NEED OF WORK

After the study of various encryption algorithms, the concept of keys has been successfully observed from the observation it has been seen that better secured system can be achieved by increasing the key length. Longer key lengths consume more power and dissipate more heat. Basically it is a tradeoff, between security and overheads. In order to achieve more secured system continuous efforts are required. An efficient encryption algorithm should consist of two factors – fast response and reduced complexity. By keeping the utility of encryption algorithm in secure communication it is desirable to optimize and/or improve the encryption techniques, so security overheads remains under control.

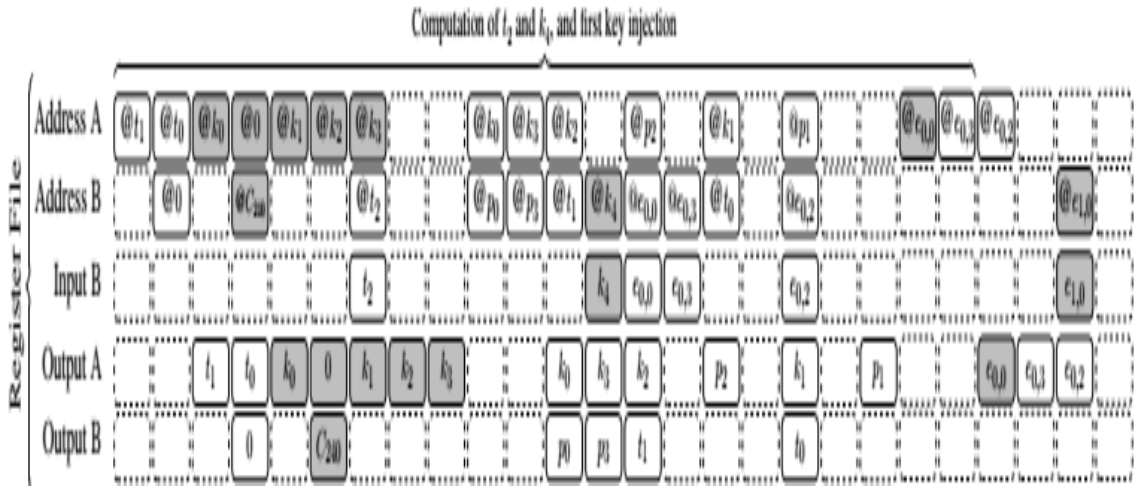
III. THREE FISH CIPHER ALGORITHM

This report discusses the three fish cipher algorithm with the help of key scheduling how the encryption does and decryption algorithms are defined by applying the plain text to encryption block and generation of cipher text as output. By applying cipher text to the decryption block and key has been scheduled in a way that deciphered text has been found.

Block Size	Number of Words (Nw)	Number of rounds (Nr)
256	4	72
512	8	72
1024	16	18

Table.1. Block size and Number of rounds

IV. KEY INJECTION SCHEDULING



V. RESULTS AND CONCLUSION

CIPHER OUT PUTS Following are simulated results of three fish block cipher algorithm implemented in virtex-5 kit with the help of Xilinx ISE 12.1.

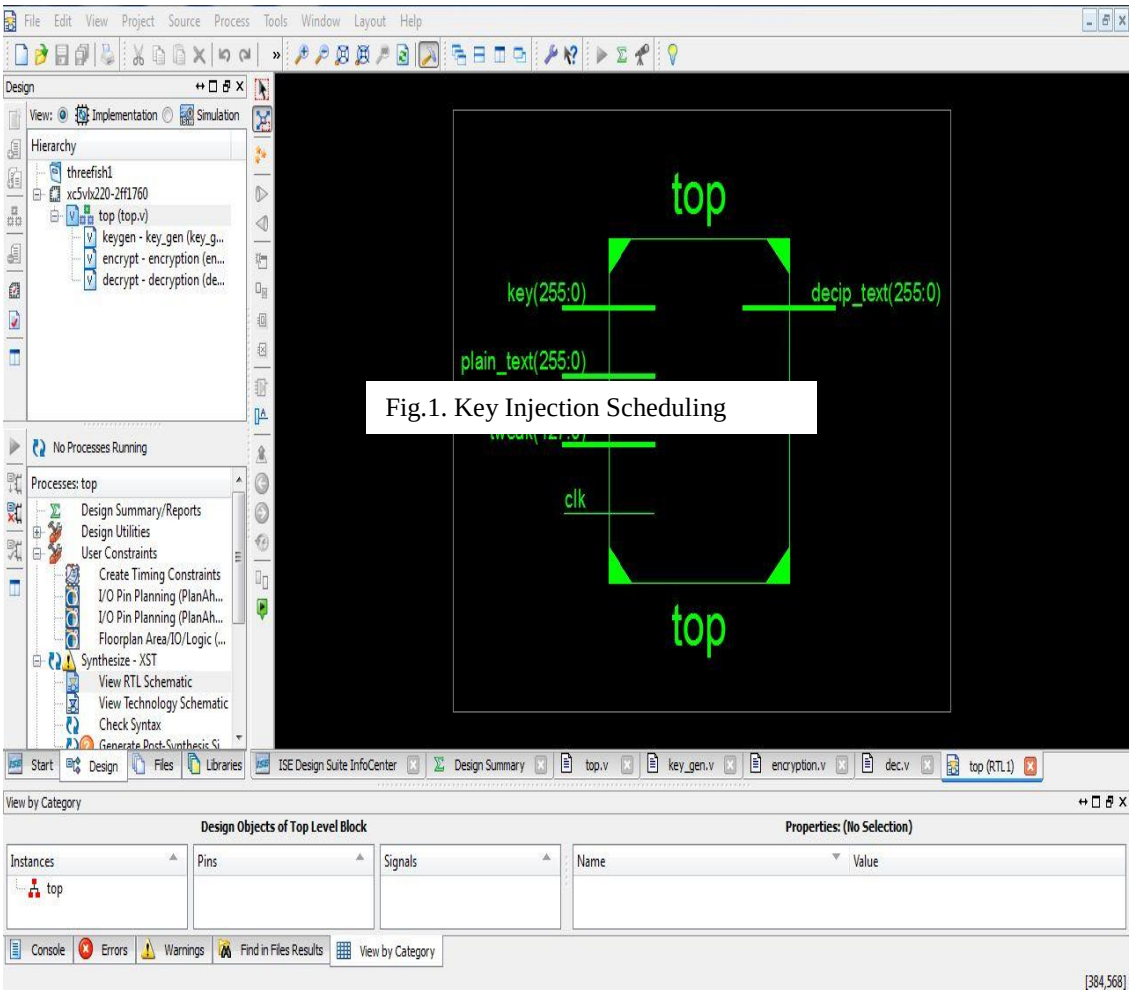


Fig.1. Key Injection Scheduling

CIPHERED OUT PUTS

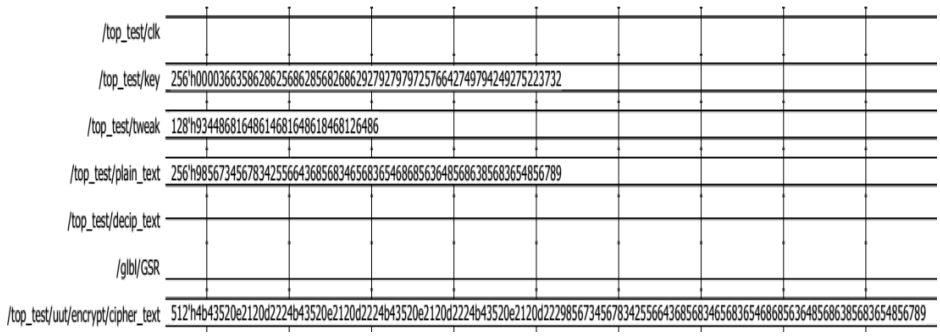


Fig.3. a) .Ciphered output

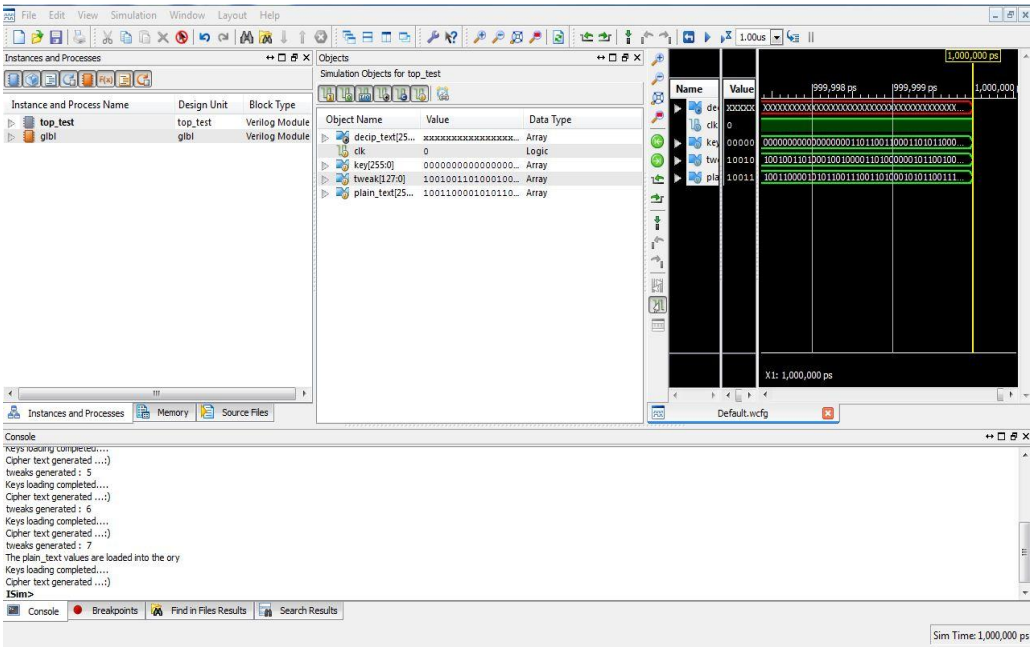


Fig. 3. b). Ciphered output

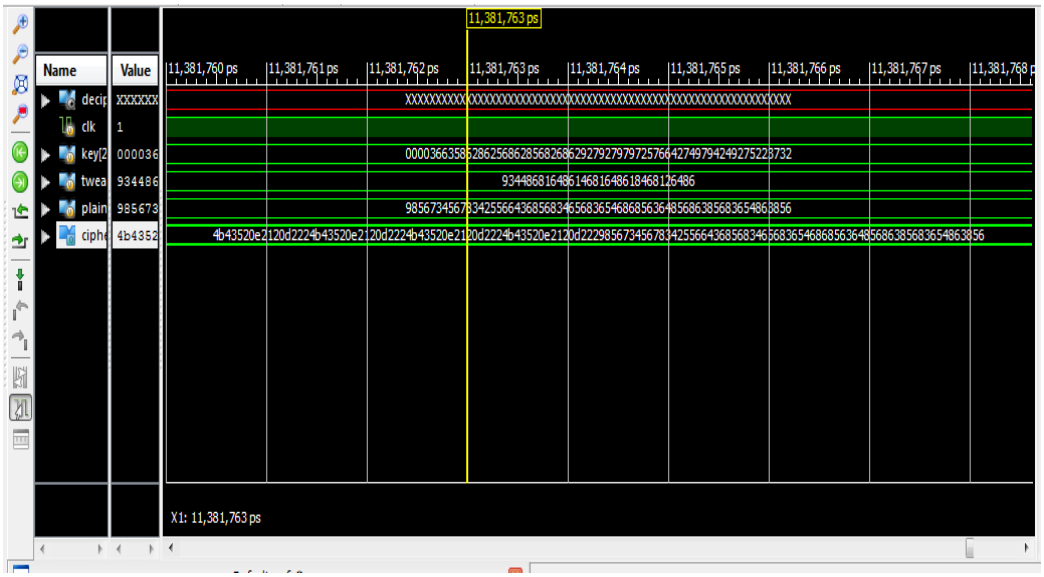


Fig. 3. c). Ciphered output

VI. CONCLUSION

- It has been noted that 14.2ns for 256 bits of input data and is very low compared to 128 bits AES encryption standard.
- The improvement has been observed to be 45.78% as compared to classical DES technique.
- The key length can be reduced, keeping the same security, in order to optimize the utilization of resources.
- The few gaps have been covered but still a lot of work can be done for the increase in security of the data along with the optimization of resources.

REFERENCES

[1]. Niels Ferguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, Jesse Walker, "The Skein Hash Function Family (Version 1.3)", Oct 2010.

[2]. D. Kahn: The Code breakers: the story of secret writing, MacMillan publishing,1996.W.Diffie and M. Hellman, "New Directions in Cryptography", IEEE Transaction on Information Theory, Vol. IT-22, 1976, pp. 644-654.

[3]. Ruth M. Davis, "The Data Encryption Standard", Proceedings of Conference on Computer Security and the Data Encryption Standard, National Bureau of Standards, Gaithersburg, MD, 1977, NBS Special Publication 500-527, pp 5-9.

[4]. Whitfleld Diffie, "Cryptographic Technology: Fifteen Year Forecast" Reprinted by permission AAAS, 1981 from Secure Communications and Asymmetric Crypto Systems. AAAS Selecte8 Symposia. Editor: C.J. Simmons. Vol. 69, West view Press, Boulder, Colorado, pp 38-57.

[5]. Ingrid Verbauwhede, "Security and Performance Optimization of a New DES Data Encryption Chip", IEEE journal of Solid-State Circuits, Vol. 23, No. 3.1988, pp 647-656.

[6]. James E. Katz, "Social Aspects of Telecommunications Security Policy", IEEE journal Technology and Society Magazine, 1990, pp 16-24.

[7]. H. Bonnenbergt, "VLSI Implementation of a New Block Cipher", IEEE journal on Information Theory 1991, pp 510-513.

[8]. K.H. Mundt, "SUPERCRYPT, ASIC Technology facilitates a new Device Family for Data Encryption", IEEE journal on cloud computing 1992, pp 356-359.

[9]. C. Boyd. "Modern Data Encryption," Electronics & Communication Engineering Journal on data security and neural networks 1993, Vol. 5, pp 271-278.

[10]. R. Zimmermann, "A 177 Mb/s VLSI Implementation of the International Data Encryption Algorithm", IEEE Journal of Solid-State Circuits. Vol. 29, No. 3, 1994, pp 303-307.

[11]. Stefan Wolter "On the VLSI Implementation of the International Data encryption Algorithm IDEA", IEEE journal on computer system and data security 1995, pp 397-400.

[12]. Seung-Jo Han, "The Improved Data Encryption Standard (DES) Algorithm" IEEE journal on information system 1996, Vol. 3, pp 1310-1314.

[13]. Hassina Guendouz, "Rapid Prototype of a Fast Data Encryption Standard with Integrity Processing for Cryptographic Applications", IEEE transaction on data originations 1998,pp 434-437.

[14]. K. Wong, "A Single-Chip FPGA Implementation of the Data Encryption Standard (DES) Algorithm" Global Telecommunications Conference, 1998. GLOBECOM 98, IEEE, Vol. 2, pp. 827-832.

[15]. M.P. Leong, "A Bit-Serial Implementation of the International Data Encryption Algorithm IDEA", 2000 IEEE conference Symposium on Field-Programmable Custom Computing Machines, pp 122-131.

[16]. R. G. Sixel, "A High Level Language Implementation of the Data Encryption Standard and a Bit-Slice Architecture", Roc 43rd IEEE Midwest Symposium on Circuits and Systems, Lansing MI, 2000, pp 266-269.

[17]. Teo Pock Chueng, "Implementation of Pipelined Data Encryption Standard (DES) Using Altera CPLD", TENCON 2000 Proceedings, Vol. 3, IEEE 2000, pp 17-21.

[18]. Yeong-Kang Lai, "A Novel VLSI Architecture for a Variable-Length Key, 64-Bit Blowfish Block Cipher", Signal Processing Systems, 1999 IEEE Workshop, pp 568-577.

[19]. Toby Schaffer, "A Flip-Chip Implementation of the Data Encryption Standard (DES)", IEEE1997, pp 13-17.

[20]. Cameron Patterson, "High Performance DES Encryption in Vertex FPGAs using Jbits", journal Symposium on FPGA 2000, pp 113-121.

[21]. Cameron Patterson, "High Performance DES Encryption in Vertex FPGAs using Jbits", IEEE journal Symposium on FPGA 2000, pp 113-121.