International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Efficient VLSI Architecture for Modified Blowfish Algorithm for Military Applications

Mushfiqua Yamen[1], Dr. M. Vadivel[2]
[1]*PG Scholar,* [2]*Associate Professor, Department of E.C.E, Vidya Jyothi Institute of Technology, Hyderabad, India.*

Abstract: ***In this paper, an Efficient VLSI architecture for modified blowfish algorithm for military applications is proposed. Security now-a-days is most challenging traits in internet and network applications. The exchange of data over the internet is increasing day by day. The work done is for network security and military applications. In the proposed blowfish algorithm security is increased by increasing the key bit size from 448-bitkey to 512-bit key and reduction of ROM size from 1024-bit to 512-bit. The design simulations are done in Xilinx ISE software by using Verilog language. The performance is analyzed in terms of area, throughput and power consumption.***
Keywords: Modified Blowfish Algorithm, Cryptography, Advanced encryption standard.

I. INTRODUCTION

Cryptography is defined as an art of creating a method to disguise information from readable form to non-readable form [2]. Basically cryptography consists of two operations, Encryption and Decryption. A known message/text called as a plaintext, is disguised by means of encryption. The disguised text is then converted back to plaintext by using decryption operation. Both the operations are carried out using a secret code usually known as a key. The sender uses a key to encrypt the message and the receiver uses the key to decrypt it. The longer the key size, security provided to the system is more. As Cryptography is a secured method of protecting information, apart from civilians the military as well as government prefer it the most.
One of the example for military based applications is BEU (bulk encryption standard). This device is developed jointly by L&T and DRDO and has the following features like it sends confidential data securely and enables completely secure data transfer of sensitive information. BEU is a high performance encryption platform that provides maximum end-to-end security. Any encryption algorithm with a private key can be used. It also provides software security through Anti-cloning IC and the complete design is based on FPGA.

II. LITERATURE SURVEY

A. DES

Data Encryption Standard is a symmetric key block cipher. It uses 64-bit as plaintext i.e., input and the output obtained is also 64-bit. In DES the key length is only 56-bits and consists of 16 rounds [3]. It is the most widely used algorithm before AES, and Blowfish algorithms. As the key length is small it is an insecure algorithm when compared to AES and Blowfish.

B. AES

Advanced Encryption Standard is more popular and widely used symmetric encryption algorithm. AES algorithm is 6x times faster than triple DES [3]. It uses 128-bit as plaintext and has 3 variable key lengths i.e., 128-bits, 192-bits and 256-bits and the no of rounds in AES depends on the key length i.e., 10, 12, 14 rounds respectively. DES is replaced with AES as its key length is too small and insecure [4].

C. Blowfish

Blowfish is a symmetric block cipher effectively used for encryption and protecting data. It has a variable key length from 32-bits to 448-bits. Blowfish was designed by Bruce Schenier in 1993 as a substitute to existing algorithms. It is a 16 round fiestal network. It operates in two modes, Key expansion mode and Data encryption mode. The role of key expansion part is to converts a key of at most 448 bits into several sub key arrays totaling 4168 bytes [6].
In this paper [7], the selected algorithms are AES, Blowfish and DES. By using these algorithms the performance of encryption and decryption process of text files is calculated through the throughput parameter. Blowfish is used in wide range of applications such as bulk encryption of data files [8], this study evaluates two commonly used symmetric encryption algorithms such as Blowfish [4] and Rijindael [5]. It was identified from [6], [7] that AES operates faster and more efficient than other symmetric encryption

algorithms. A study in [8] is conducted for different popular secret key algorithms such as DES, DES, AES, and Blowfish. DES when compared to AES it is found that AES is more effective in terms of throughput, power consumption and more security levels as it has variable key lengths. AES is a complex algorithm which consumes more area and power and hence to reduce that Blowfish algorithm is used.

Section-2 will provide the information about the proposed blowfish algorithm and modified Blowfish Algorithm. Section-3 will give a brief discussion about the methodology used with the simulations. Section-4 will discuss about the simulation results and section-5 completes this paper by briefing the key points and other related concerns.

III.PROPOSED ALGORITHM

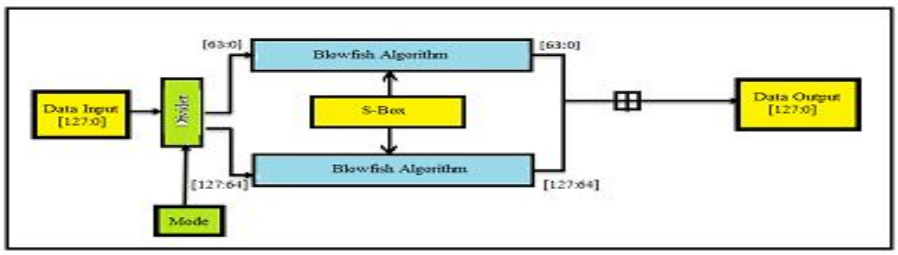

Fig.1. Block diagram of proposed blowfish algorithm

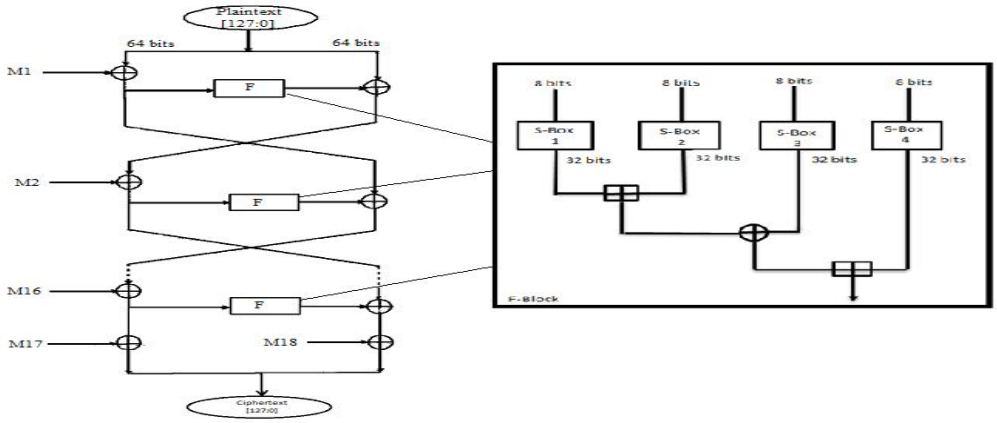

Fig.2. Blowfish algorithm with F function

Blowfish is a symmetric block cipher effectively used for encryption and protecting data. It has a variable key length from 3bits to 448-bits. It was designed by Bruce Scheiner in1993 as an alternative to other existing algorithms. Blowfish is a 16-round fiestal network. It operates in two modes, key expansion and data encryption mode. Mode is used to change the encryption or decryption standard.

The role of key expansion mode is to alter a key of at most 448 bits into several sub key arrays totaling 4168 bytes. Data encryption mode takes place through a 16-round fiestal network. Each round consists of F function. A plaintext of 128-bits is given as input to the blowfish algorithm. The 128-bit under goes encryption and decryption. The plaintext of 128-bits is divided into 64-bits each. 64-bits undergoes encryption first. It is sub divided into 32-bits each i.e.; LSB bit and MSB bit. Key (M1, M2, .M18) is given along with plaintext.

The MSB bit is XORed with the key i.e.; M1 and the XORed output value obtained is 32-bits given to the F unction. The F unction basically known as fiestal function consists of 4 s-boxes in it. It takes four 8-bits as inputs each, and are XORed. The output obtained from the F function is 32-bits again and it is XORed with another LSB bit. The value obtained by XORing the LSB bit is given to the MSB bit for the next round and XORed with the key i.e.; M2 and so on. Blowfish algorithm has 16 rounds with F function and the last two rounds are without F function in order to get the cipher text i.e.; M17, M18. The obtained cipher text is again decrypted in order to get the plaintext.

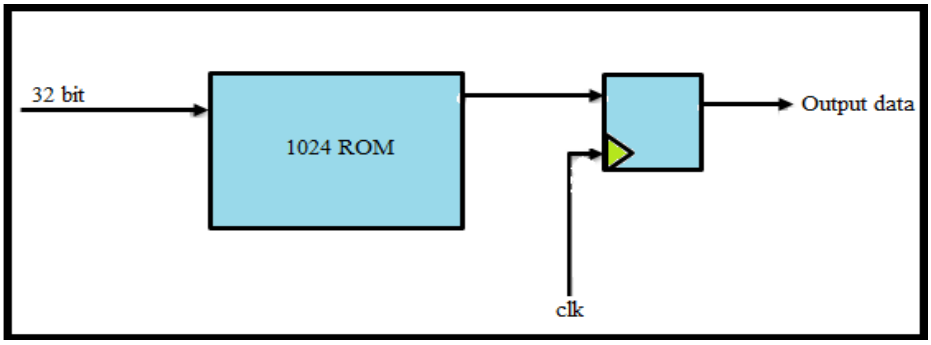

Fig.3. Proposed memory based method

In the proposed blowfish algorithm only 14 rounds are used for encryption and decryption process. 128-bit is taken as plaintext along with 448-bit key size and 1024 ROM as shown in fig3.

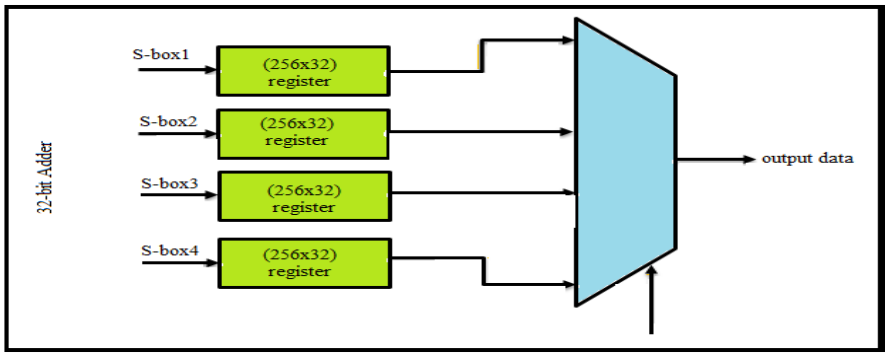

Fig.4. Proposed s-box register

The proposed method is compared with the S-box method invented by [12] as shown in Fig.4, since their output results are the best among others. The 256 × 32-bit registers are utilized for every S-boxes. Each register has a clock, input data, and output data, and it enables a signal port. The 32-bit input information of addr are latched and put away inside for each clock cycle. This method can back off the speed of the Blowfish execution as each register has its own timing delay.

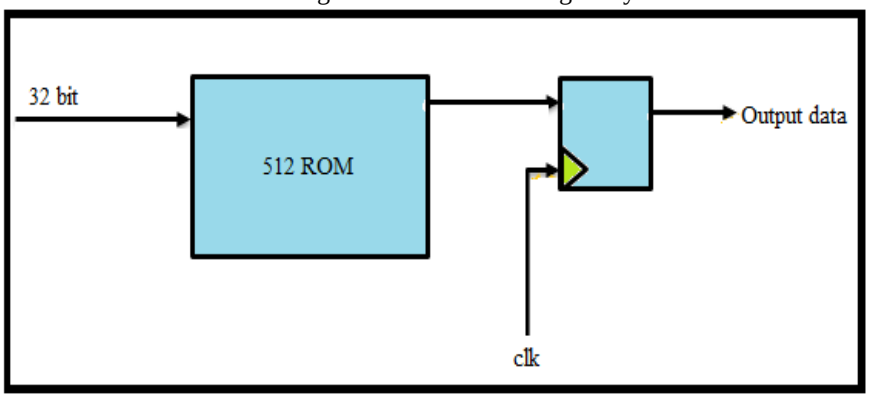

Fig.5. Modified 512 ROM

In the modified blowfish algorithm, the key size is increased from 448-bit to 512-key and the ROM size is reduced from 1024 to 512 which contributes in reducing the area, power consumption etc. Usually blowfish consists of 18 rounds in which 16 rounds are performed using Fiestal block cipher and the last two rounds are used to get the cipher text. Earlier in the proposed algorithm only 14 rounds were used an in existing blowfish algorithm 16 rounds are used. By increasing the key size the security provided to the system is more.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

IV. INSIGHT OF MODIFIED BLOWFISH ALGORITHM

The operation inside the blowfish algorithm can be explained using an example as shown below. Following fig shows operation of one single round.

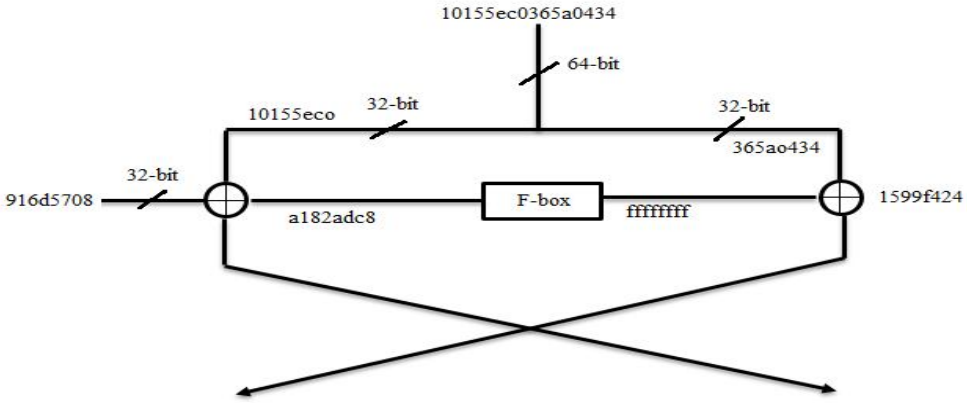

Fig.6. Single round operation of blowfish algorithm

Let us consider a 64-bit of plaintext Z (10155ec0365a0434) is given as input. It is divided into two 32-bits each i.e.; A (10155ecO), B (365a0434) respectively. A key of 32-bits i.e.; (916d5708) is given along with the input. The MSB bit A is now XORed with the key and the output value obtained is (a182adc8) given to the F function where the s-boxes undergoes XOR and MOD operations and the s-box output is (ffffffff) now XORed with the another LSB bit B and the final output value obtained from the first round is (1599f424) is transferred to the MSB bit side as LSB bit is not XORed with the key and so on.

V. SIMULATION RESULTS

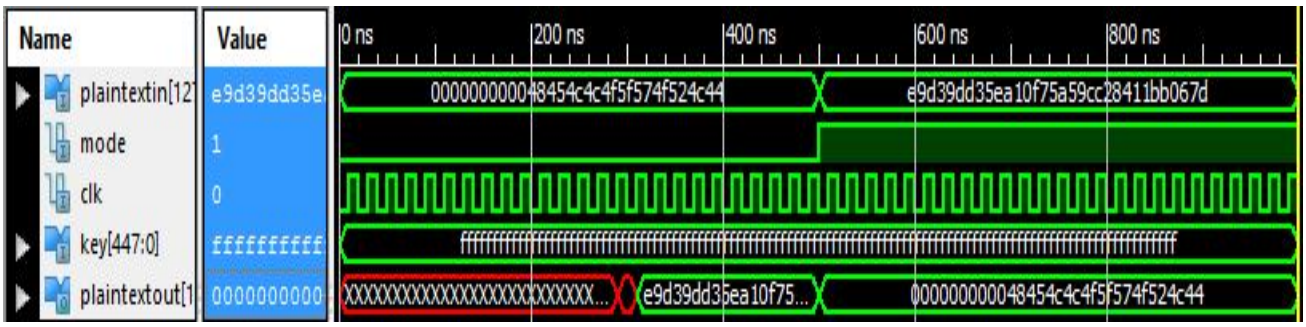

Fig.7. Simulation results for existing 448-bit key

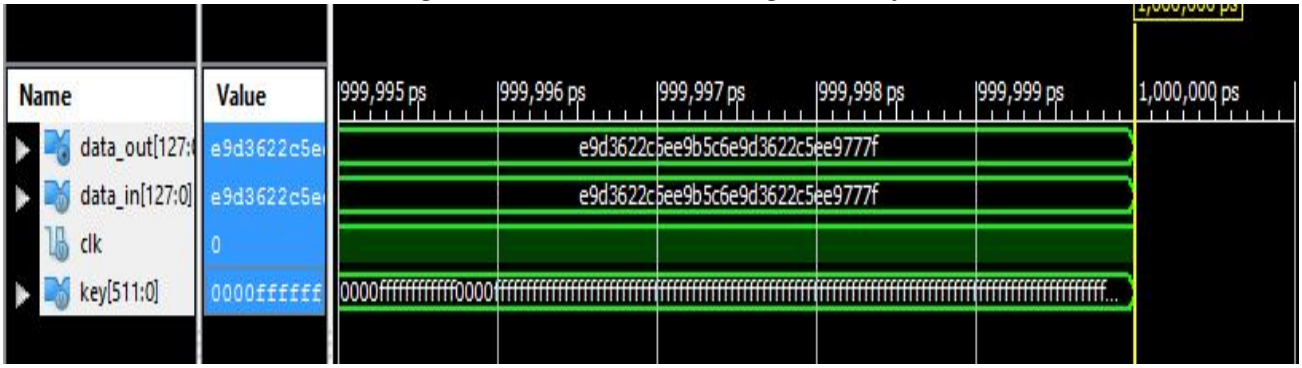

Fig.8. Simulation results for proposed 512-bit key

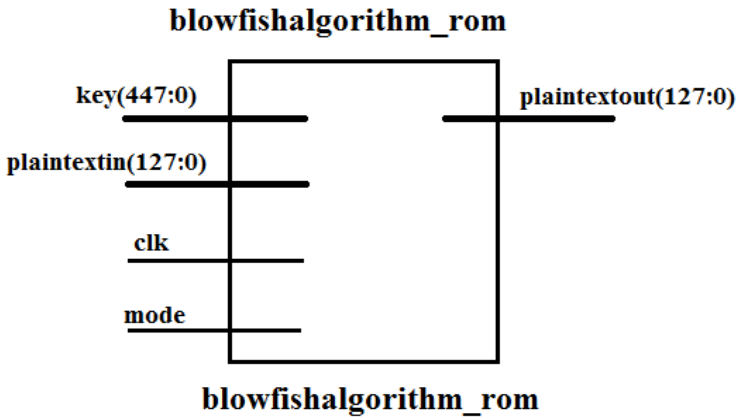

Fig.9. RTL schematic for existing blowfish

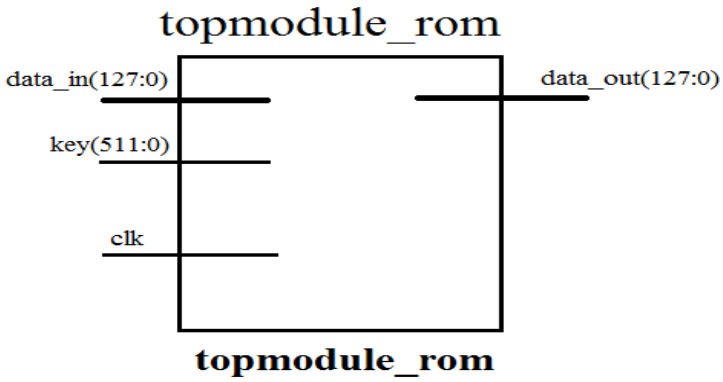

Fig.10. RTL schematic for proposed blowfish

Table 1: comparison table for existing and proposed blowfish algorithm in terms of synthesis report.

PARAMETERS		Existing BLOWFISH with 448-bit key 1024 ROM	Proposed BLOWFISH with 512-bit key 512 ROM
SYNTHESIS REPORT	No of slice registers	1116	1126
	No of slice LUT'S	2218	2228
	No of bonded IOBs	161	161

In the above given table the parameters are analyzed by using spartan3E (3s1200efg320-4). The throughput can be calculated as Throughput (Gbps) = 128 bits * clock frequency (MHz) / Latency.

Table 2: comparison table of existing and proposed blowfish algorithm in terms of area, throughput and delay

PARAMETERS	Existing BLOWFISH with 448-bit key & 1024 ROM	Proposed BLOWFISH with 512-bit key & 512 ROM
Delay	9.041ns	8.041ns
Throughput	6331.957mbps	10434.49mbps
Power consumption	0.168W	0.158W

VI.CONCLUSIONS

This paper presents performance analysis of area, throughput and power consumption for blowfish algorithm. The area as well as the power consumption is reduced and the throughput is obtained is high. Simulation results shows that the encryption and decryption are performed using blowfish algorithm making it an alternate for AES, DES algorithms. The security is increased by increasing the key size from 448-bit to 512-bit and area is reduced by reducing the ROM size from 1024 to 512.

REFERENCES

[1] Sai Kumar Manku and K. Vasanth, “Blowfish Encryption Algorithm for Information Security,” ARPN Journal of Engineering and Applied Sciences, VOL. 10, NO. 10, JUNE 2015.
[2] S. Sukumar, Raghuram, Chaitali, and Chakrabarti, “Programmable processor for cryptography,” in Proceedings of IEEE International Symposium on Circuits and Systems. Geneva, Switzerland, 2000, pp. 685-688.
[3] Xinmiao Zhang Parhi, K.K. “Implementation approaches for the Advanced Encryption Standard algorithm”, IEEE Circuits and Systems, 2[4], 2002.
[4] R. Chandramouli, "Battery power-aware encryption - ACM Transactions on Information and System Security (TISSEC)," Volume 9, Issue 2, May. 2006.
[5] S.Hirani, "Energy Consumption of Encryption Schemes in Wireless Devices Thesis," university of Pittsburgh, April 9, 2003. Retrieved October 1, 2008.
[6] “Performance Analysis of AES and BLOWFISH Algorithms “, National Conference on Computer Communication & Informatics”, School of computer science, RVS college of arts and science, March 07, 2012.
[7] Shashi Mehrotra Seth, Rajan Mishra, “Comparative Analysis of Encryption Algorithms for Data Communication”, IJCST Vol.2, Issue 2, June 2011.
[8] Tingyuan Nie Teng Zhang,” A study of DES and Blowfish encryption algorithm”, Tencon IEEE Conference, 2009.
[9] Nadeem, A.; Javed, M.Y, "A Performance Comparison of Data Encryption Algorithms," IEEE Information and Communication Technologies, 2005. ICICT 2005. First International Conference, 2006-02-27, PP. 84- 89.
[10] Pooja B. Optimization of Cryptography Algorithms in Cloud Computing. International Journal of Computer Trends and Technology. 2017; 46(2):67-72.
[11] Sinha, S., Islam, S. H., & Obaidat, M. S. (2018). A comparative study and analysis of some pseudorandom number generator algorithms. Security and Privacy, 1(6), e46.
[12] P. Princy, A Comparison Of Symmetric Key Algorithms DES, AES, Blowfish, RC4, RC6: A Survey”, International Journal of Computer Science & Engineering Technology (IJCSET), Vol. 6 No. 05, May 2015.
[13] Shraddha D. Performance Analysis of AES and DES Cryptographic Algorithms on Windows & Ubuntu using Java. International Journal of Computer Trends and Technology. 2016; 35(4):179-183.