Synthesis and Analysis of 64-Bit Blowfish Algorithm Using VHDL

Viney Pal Bansal[1,a], Parminder Singh Jassal[2,b]

[1]M.Tech student,ECE section, Yadavindra College of engineering, Talwandi Sabo, India
[2]Assistant professor,ECE section, Yadavindra College of engineering, Talwandi Sabo, India
E-mail: [a]Vineybansal555@gmail.com, [b]pammi_jassal@yahoo.co.in

Abstract. Data security has become the major issue now in these days, especially for the use of internet. So, to protect the IP-based data, we must have to use strong cryptographic techniques. Blowfish cryptosystem is one of the strong and fast algorithms used for cryptography. This paper presents the implementation of Blowfish algorithm using VHDL. The device Virtex 4 is used with Xilinx ISE 14.1. The device utilization is improved by 1% and delay is reduced by 2ns in this work.

Keywords: Encryption, Blowfish, FPGA, VHDL, Internet.

1. Introduction

Cryptography for Data security is a very powerful method for protection of data from being stolen. Cryptography is a method to encode the information to keep the information from being hacked by the other party [1]. Cryptography has two methods, one is symmetric and another one is asymmetric. In Symmetric cryptography, same key is used and share for both Encryption and Decryption. And, in asymmetric cryptography, different keys are used for Encryption and Decryption. Symmetric cryptography is simple in structure, so widely used. Blowfish is an example of Symmetric cryptography. Blowfish is a license free algorithm and not yet cracked.

2. Reason For Use

2.1. VHDL

Mostly, for FPGA boards, VHDL is commonly used. It uses high level modeling for constructs. The concept of packages in VHDL, library management and separate compilation makes it an ideal candidate for higher level system modeling. There is no concept of packages in Verilog. Functions and procedures used within a module have to be defined inside the same module and thus they cannot be shared by different modules. However, the concept of package in Verilog may be emulated by declaring and instantiating a fictitious module with functions and procedures.

3. Related Work

To get familiar with Blowfish algorithm, there are some other works from related field, which shows the performance of Blowfish algorithm.
In [1], research presented the performance of blowfish algorithm with total time taken for encryption, avalanche effect and throughput from multiple testing scenarios as the parameters. The Blowfish algorithm was implemented on FPGA using VHDL language. The results showed that reducing the rounds of Feistel reduce total encryption time, give greater throughput and not affect avalanche effect significantly. It also showed that larger key length needs more resources to implement on FPGA. Finally, blowfish algorithm was implemented on FPGA Virtex-4 XC4VLX25-SF363 well.

In [2], authors analyzed two symmetric key encryption algorithms: DES (data encryption system) and Blowfish. They analyzed the security for both. Authors evaluated encryption speed and power consumption for their performance. Experimental results showed that Blowfish algorithm runs faster than DES algorithm while both of them consume almost the same power. It is proved that Blowfish algorithm maybe more suitable for wireless network which exchanges small size packets.
In [5], the popular secret key algorithms including DES, 3DES, AES (advanced encryption system), Blowfish, were implemented, and their performance was compared by encrypting input files of varying contents and sizes. The algorithms were implemented on two different hardware platforms, to compare their performance. In the end, the results were presented which conclude that the Blowfish is the fastest algorithm. Though security was not catered for, in practice, however, one would consider the security first.
In [6], the selected encryption algorithms namely DES, AES and BLOWFISH are used for performance evaluation in this paper. Based on input size of text files and experimental result, it is conc1uded that Blowfish algorithm consumes less execution time, memory usage and produces more throughputs. Blowfish performs approximately 4 times faster than AES and 2 times faster than DES. Blowfish consumes less memory compared with AES and DES. AES showed poor performance results compared to other algorithms, since it requires more processing power. Blowfish is not only fastest but also provides the great security through strong key size which enables it to be used in many applications like Bulk Encryption, Random Bit Generation, Internet based Security, Packet Encryption and so many applications.

4. Design of Algorithm

The block diagram of Blowfish algorithm is shown in figure below:

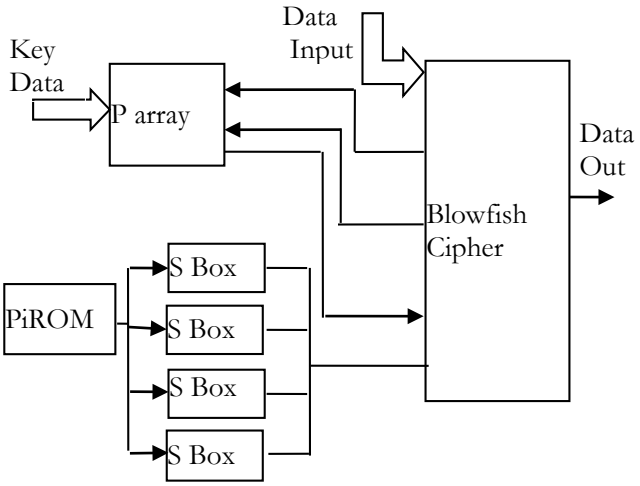

Fig. 1. Block Diagram of Blowfish Algorithm

Blowfish algorithm is a symmetric block cipher which consists two parts:

4.1. Key Expansion

- Initialize first the P-array (32-bits) and then the four S-boxes with 256 entries each of 32-bits hexadecimal digits [3].
- XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits. (For short key, there is at least one equivalent longer key. As, if A is a 64-bit key, then AA, AAA, etc., are equivalent keys).
- Encrypt the all-zero string with the Blowfish algorithm, using the subkeys.
- Replace P1 and P2 with the output of step (2).
- Encrypt the output of step (3) using the Blowfish algorithm with the modified subkeys.

- Replace P3 and P4 with the output of step (4).
- Continue the process, replacing all entries of the P-array, and then all four S-boxes in order, with the output of the continuously-changing Blowfish algorithm.

4.2. Data Encryption

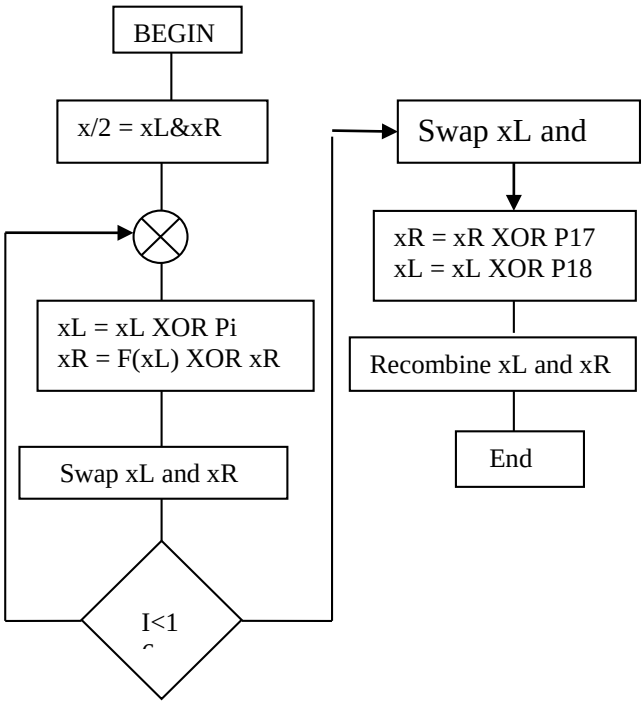

Fig. 2. Flowchart for data encryption

5. Previous Work

In [1], Blowfish was implemented on FPGA virtex-4 XC4VLX25-SF363 using VHDL. There is limited no. of resources available on FPGA virtex-4 XC4VLX25-SF363. There are only 240 input/output pins provided on this FPGA board. The algorithm uses 64 inputs (plaintext) and 64 outputs (ciphertext) and 9 control pins. So, 137 out of 240 pins are used by design. There are only 103 pins left for input key. Only 64 bit input key was used.

5.1. Avalanche Effect

The avalanche effect was calculated by no. of different ciphertext from the plaintext for various key lengths. It has the same plaintext with different sizeand different value of the key length. The avalanche effect refers to adesirable property of cryptographic algorithms, whenan input is changed slightly the output changessignificantly. It analyzed that the difference of keylength had no effect in avalanche effect. The averageavalanche effect for this work is about 50%.

5.2. Changing key Size

The IOB is pin resources needed to implement the designin FPGA. The design takes 64 inputs (plaintext), 64 Outputs (ciphertext) and 9 control pins. So, total 137pins are needed without considering input key. XC4VLX25 SF363 contains 240 IOB pins. Therefore, the key lengthmust be less than 103 pins. So, only 64 bit key lengths were used in this workimplemented in FPGA.

6. This Work

In this paper, the implementation of Blowfish algorithm using VHDL is presented. The key size is 64 bits as Virtex 4 XC4VLX25 has 240 bits of IOB pins. The algorithm uses 64 bits input text and 64 bits output cipher and 9 control pins are used in the algorithm. So, 103 IOB pins remained for input keys. Thus, only 64 bits key is used for implementation.

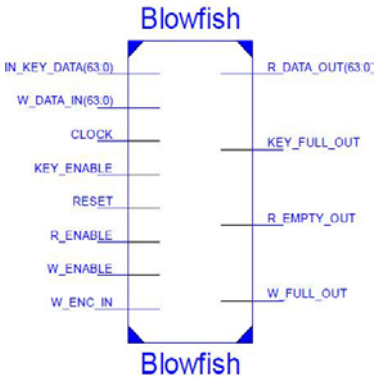

Fig. 3. RTL schematic of 64 bits Blowfish algorithm

Table 1. Device Utilization for 64 Bits Blowfish algorithm

Source device	Prasetyo et. al [1]		our work		
Virtex 4 XC4VLX25	Used	Percentage	Used	Percentage	Available
No. of Slices	678	6%	574	5%	10752
No. of Slices Flip-flop	424	2%	420	2%	21504
No. of 4 input LUTs	1024	5%	1093	5%	21504
No. of Bounded IOB	201	83%	201	83%	240
No. of FIFO 16	7	9%	7	9%	72

The results in the table shows that device utilization is less than devices utilized in [1]. Minimum period: 7.933ns (Maximum Frequency: 133.233MHz). Minimum input arrival time before clock: 4.550ns. Maximum output required time after clock: 7.351ns. Maximum combinational path delay: 6.350ns. It clearly shows that presented work has better implementation results than the previous work.

6.1. RTL schematic for 128 bits Blowfish algorithm

The device virtex-4 XC4VSX25-FF668 is referenced for implementation of algorithm. This board provides 320 input/output pins instead of 240 pins available on XC4VLX25-SF363. So, the security of algorithm increases and vulnerability to Brute force attack reduces as input key varying from 32 bits to 160 bits. Also, the device utilization is improved by 1% of Blowfish algorithm design.

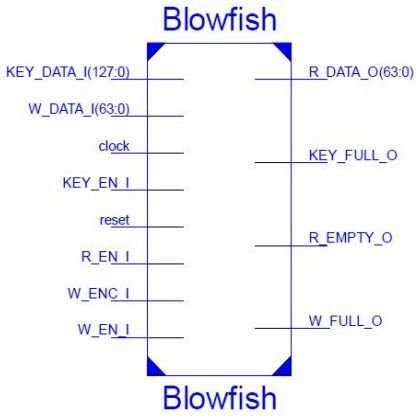

Fig. 4. RTL schematic of 128 bits Blowfish algorithm

Table 2. Device Utilization for 128 Bits Key

Source device Virtex 4 XC4VSX25	Used	Percentage	Available
Slices	627	5%	10240
Slices Flip-flop	484	2%	20480
4 input LUTs	1127	4%	20480
Bounded IOB	265	82%	320
FIFO 16	7	5%	128

Minimum period: 8.08ns (Maximum Frequency: 128.072MHz). Minimum input arrival time before clock: 4.550ns. Maximum output required time after clock: 7.328ns. Maximum combinational path delay: 6.350ns.

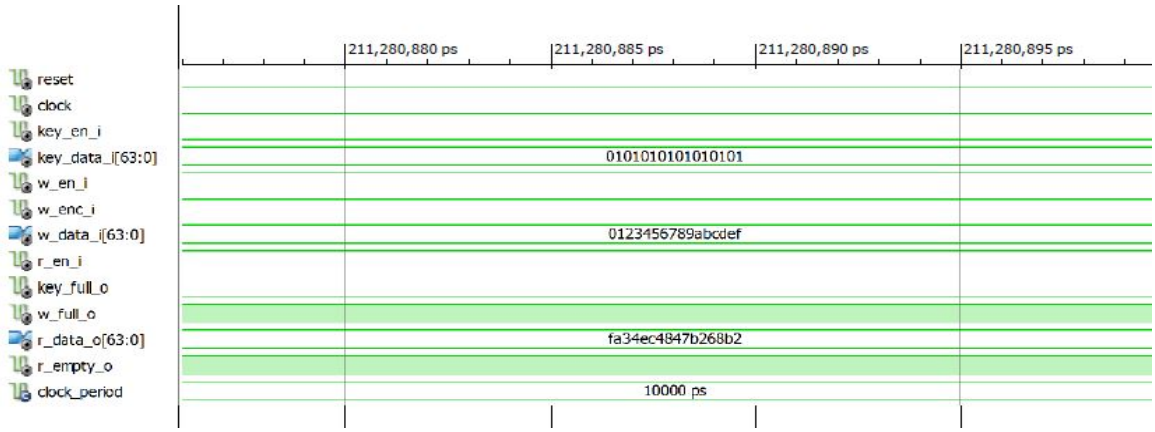

Fig. 4. Simulation waveform of encryption using 64 bit Blowfish algorithm

The Simulation waveforms for decryption of Blowfish algorithm are shown in figure below:

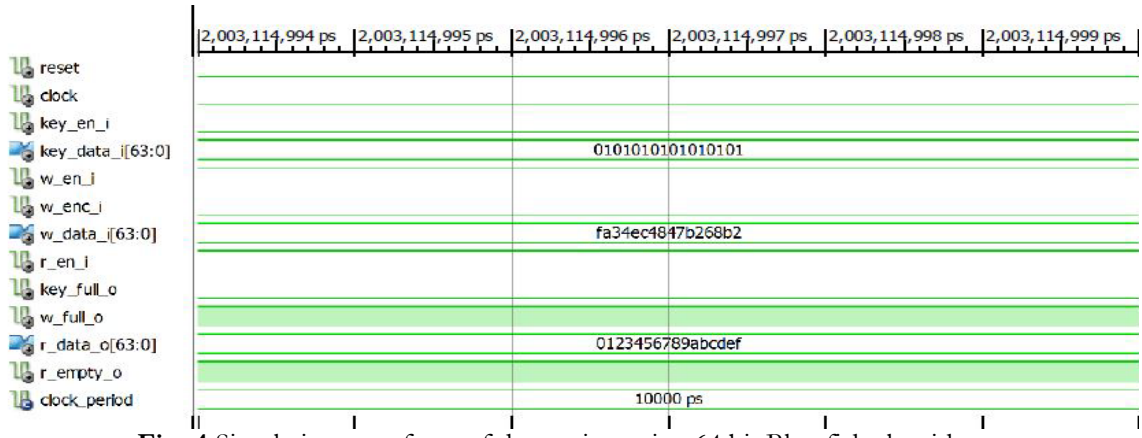

Fig. 4. Simulation waveform of decryption using 64 bit Blowfish algorithm

The implemented algorithm is tested for all the test vectors defined for Blowfish algorithm and found true for all the test vectors.

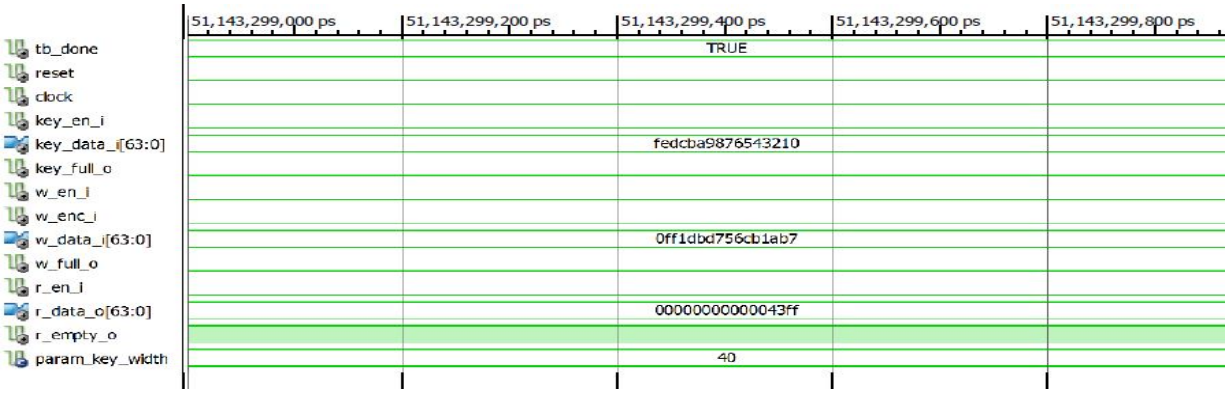

Fig.5. simulation waveform for test vectors

7. Conclusion and Future Scope

This research presents the implementation of Blowfish algorithm using VHDL. The implemented design consumes fewer devices available on board which results better performance of algorithm. The delay is also reduced by using shortest coding path for each block of design. The length of key input is increased so reduces vulnerability to brute force attack. Finally, the Blowfish algorithm is implemented.

For the Future work, it is recommended that the input and plaintext is replaced using image or audio/video data. It is recommended to use FPGA device which better specification than Virtex-4 XC4VSX25-FF668 which has more no. of input/output pins. The modification of blowfish algorithm can be done to get better security or reduces total encryption time.

References

[1] Prasetyo, K.N.; Purwanto, Y.; Darlis, D., "An implementation of data encryption for Internet of Things using blowfish algorithm on FPGA," *International Conference on Information and Communication Technology*, vol. no. 2, pp.75-79, 28-30 May 2014.

[2] TingyuanNie; Chuanwang Song; XulongZhi, "Performance evaluation of DES and Blowfish algorithms," *International Conference on Biomedical Engineering and Computer Science*, vol., no. 1, pp.1-4, 23-25 April 2010.

[3] Bruce Schneier, "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)", *Lecture Notes in Computer Science*, vol. no. 809, pp 191-204, 08 June 2005.
[4] Meyers, R.K.; Desoky, A.H., "An implementation of the Blowfish cryptosystem," *IEEE International Symposium on Signal Processing and Information Technology*, vol., no. 4, pp. 346-351, 16-19 Dec. 2008.
[5] Nadeem, A.; Javed, M.Y., "A performance comparison of data encryption algorithms," *International Conference on Information and Communication Technologies*, vol. no. 1, pp.84-89, 27-28 Aug. 2005.
[6] Ramesh, A.; Suruliandi, A., "Performance analysis of encryption algorithms for Information Security," *International Conference on Circuits, Power and Computing Technologies*, vol. no. 7, pp. 840-844, 20-21 March 2013.
[7] Yeong-Kang Lai; Yu-ChuanShu, "A novel VLSI architecture for a variable-length key, 64-bit Blowfish block cipher", *IEEE Workshop on Signal Processing Systems*, vol. no. 3, pp.568-577, 1999.
[8] Nayaka, R.J.; Biradar, R.C., "Key based S-box selection and key expansion algorithm for substitution-permutation network cryptography," *International Conference on Emerging Research Areas, Microelectronics, Communications and Renewable Energy*, vol., no. 1, pp.1-6, 4-6 June 2013.
[9] Gurjeevan Singh, Ashwani Kumar, K. S. Sandha, "A Study of New Trends in Blowfish Algorithm", *International Journal of Engineering Research and Applications*, vol. 1, no. 2, pp. 321-326. 2010.
[10] Chiuchisan, I., Potorac, A.D., G.A., "Finite state machine design and VHDL coding techniques" *International Conference on Development and Application Systems*, vol. no. 10, pp. 273–278, 2010.
[11] Mazumdar, B.; Mukhopadhyay, D.; Sengupta, I., "Design for Security of Block Cipher S-Boxes to Resist Differential Power Attacks," *International Conference on VLSI Design*, vol., no. 25, pp.113-118, 7-11 Jan. 2012.