International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-1 Issue-5, June 2012

Blowfish Encryption: A Comparative Analysis using VHDL

Deepak Kumar Dakate, Pawan Dubey

Abstract— Data security has always been important in all aspects of life. Data may contain several form of information that we want to secure from any unauthorized access. It can be all the more important as technology continues to control various operations in our day to day life Reprogrammable devices are highly attractive options for hardware implementations of encryption algorithms as they provide cryptographic algorithm agility, physical security, and potentially much higher performance, therefore this paper investigates a hardware design to efficiently implement a special type block ciphers in VHDL and its comparative analysis in different parameter variation . This hardware design is applied to the new secret and variable size key block cipher called Blowfish designed to meet the requirements of the previous known standard and to increase security and to improve performance. The proposed algorithm will be used a variable key size.

I. INTRODUCTION

The importance of cryptography applied to security in electronic data transactions has acquired an essential relevance during the last few years. Each day millions of users generate and interchange large volumes of information in various fields, such as financial and legal files, medical reports, and bank services via Internet, telephone conversations, and e-commerce transactions. These and other examples of applications deserve a special treatment from the security point of view, not only in the transport of such information but also in its storage so there is a need of some strong encryption algorithms to fulfill these criteria.

Blowfish Encryption Algorithm

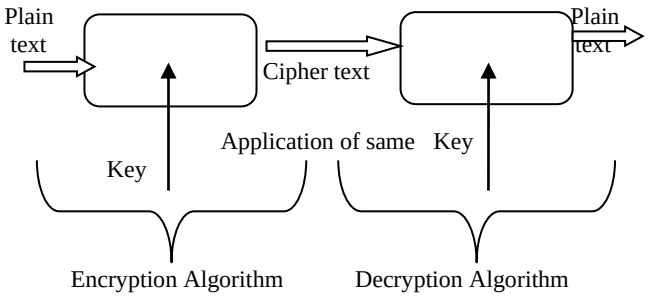

Fig1: Symmetric Encryption/Decryption Process of Blowfish Algorithm

Blowfish is one of the such kind of security treatment which applies its special kind of encryption process to secure the data in an easy and efficient way. Moreover Blowfish is a variable key size encryption algorithm which is based on block cipher technology. It is a symmetric kind of algorithm that uses same key for encryption as well as for decryption. One basic advantage of Blowfish is that it can use different key size up to the length of 448 bits.[1]

II. HARDWARE IMPLEMENTATION USING VHDL

VHDL (Very High Speed Integrated Circuit Hardware Description Language) was chosen as a language used to describe the improvement suggested to algorithm stated above. VHDL has many features appropriate for describing the behavior of electronic components ranging from simple logic gates to complete microprocessors and custom chips. Features of VHDL allow electrical aspects of circuit behavior (such as rise and fall times of signals, delays through gates, and functional operation) to be precisely described .[2]

This paper also is presenting a mix of VHDL architecture (structural and behavioral) in order to write the deign code of the encryption algorithm that describe improved blowfish algorithm. The presented architecture allows keeping the flexibility of the algorithm by taking advantage of generic VHDL coding. It executes one round per clock cycle, computes the round and the key round in parallel and supports both encryption and decryption at a minimal cost.

III. PLATFORM USED

With the help of VHDL as a description language for hardware Altera Quartus II has been used as a platform to develop the logic and for other analysis.

IV. ENCRYPTION DEVELOPMENT

As to develop the logic, key generation is one of the complex schedule of Blowfish encryption because of the fact that it includes variable size key. So for the development of the key the use of S BOX (Substitution Box) can be a greater aid for developing of logic of this algorithm.[3].

Manuscript published on 30 June 2012.
***** Correspondence Author (s)
Deepak Kumar Dakate*, Electronics and communication, Gyan Ganga College of Technology, Jabalpur, India.
Pawan Dubey, Electronics and Communication, Gyan Ganga College of Technology, Jabalpur, India.

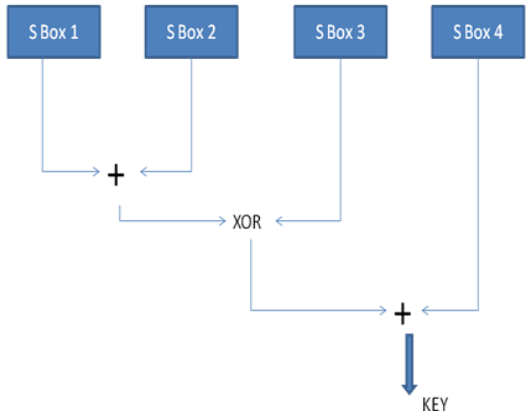

Fig2: Key Generation using Fiestel Network for Blowfish Encryption

Above figure shows the key generation concept of this particular implementation using VHDL. As we provide 8 bit input to single S Box, which outputs 32 bits data, similarly in case of rest of S Boxes the same concept to be followed. After which addition and XOR operation generates the key which is used for data encryption.

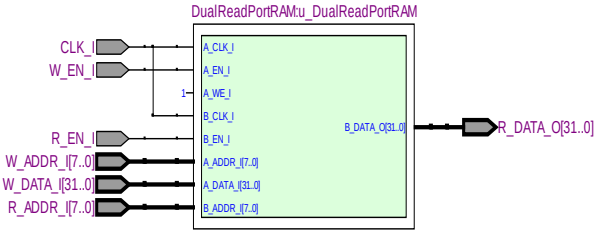

Fig3: RTL View of Single S BOX after Software Simulation.

RTL view in fig3 shows that one single S BOX can output 32 bits of data while taking 8 bit as an input, so that use of four S BOX with the logic shown in fig2 can develop a key of size 128 bits. For the development of key variation the configuration of S Boxes can be changed.[5]

This S BOX can also be simulated in Altera Quartus II software using a vector waveform file (whose screen shot is given below).This figure shows the 32bit output of single S BOX depending on 8 bit input in the form of waveform. It generates the output with application of clock input while enabling the corresponding port. With the application of internal architecture of S BOX 8bits input transfers in 32 bit output, which can be combined with outputs of other S BOXES to generate the key.

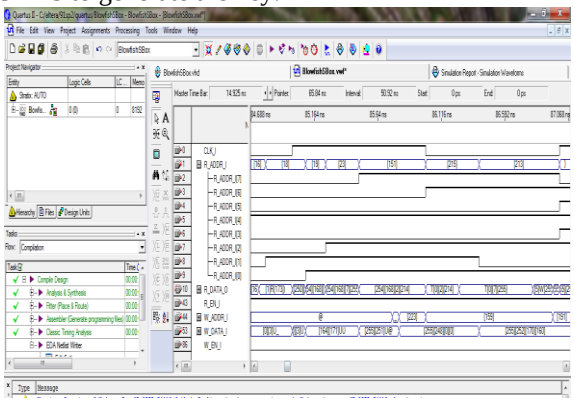

Fig4: Waveform Screenshot of Software Simulation

So with the help of generated key following process is pursued for encryption implementation

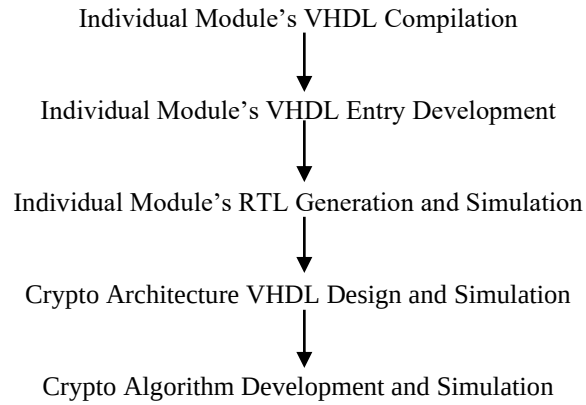

Fig5:Approach for Encryption Design.[5]

V. POWER PERFORMANCE ANALYSIS

In variable key size Blowfish algorithm the power requirement can be analysed by varying the key size under certain limit for same logic.

Table 1: Power Analysis For different Key Size

S. No.	Key Size	Core Static Power Dissipation(mW)	Input Output Power Dissipation(mW)
1	128	303.6	29.86
2	143	303.7	30.36
3	160	303.9	30.93
4	192	302.3	32.00
5	224	302.4	33.10
6	228	302.4	33.24

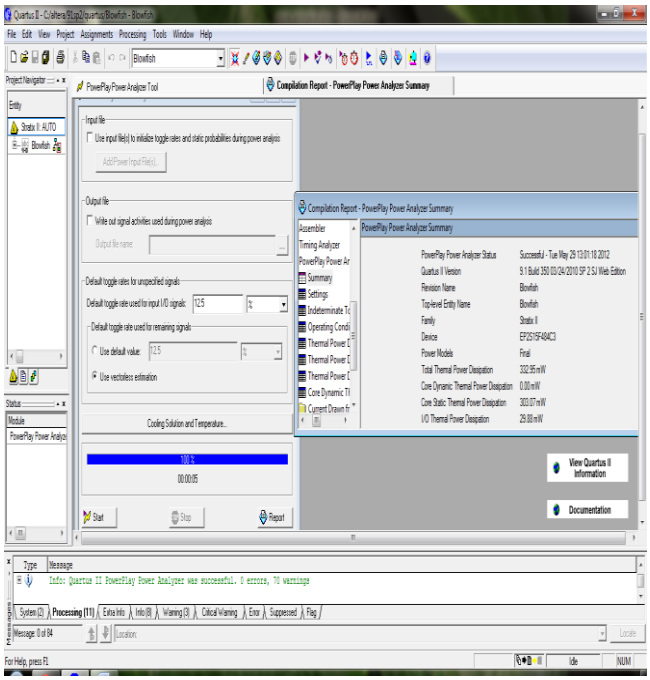

Fig6: Software Screenshot of power analysis for Key Size 128 bits.

Figure6 shows the Input Output and Core Static Power analysis for 128 bits key size. Same can be simulated for the various keys shown in the table1.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

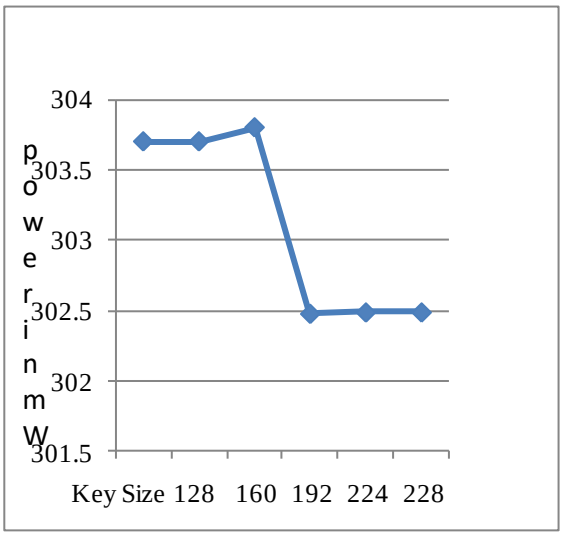

Fig7: Graphical Analysis of Core Static Power Dissipation

Figure7 demonstrate that Core Static Power Dissipation first increases with increase in key size up to a certain limit, after the limit it follows decrement and again increment with key size enhancement.

Analysis for Input Output power produces the following results.

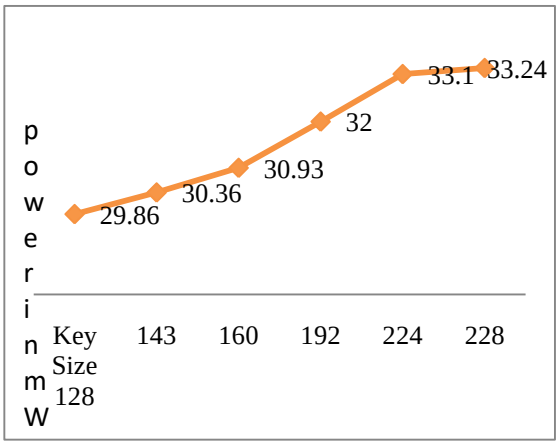

Fig:8 Graphical Analysis of Input Output Power Dissipation

VI. CONCLUSION

Above mentioned concept presented a low power, high throughput Blowfish cryptographic implementation. The proposed scheme allows 29.86 mW power for 128 bits to be dissipate input output power which is also not too much for higher key size. The results shows a trade off between security and power consumption. This paper proves that proposed technique consumes less power for lower key size.

REFERENCES

[1] B. Schneier, Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish),Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994.

[2] M. Thaduri, S.-M. Yoo, An efficient VLSI implementation of IDEA encryption algorithm using VHDL, Sciencedirect ,5 JUNE 2004.

[3] Afaf M. Ali Al-Neaimi, New Approach for Modifying Blowfish Algorithm by Using Multiple Keys, IJCSNS, March 2011.

[4] Krishnamurthy G.N , V. Ramaswamy , Leela G.H and Ashalatha M.E," Blow-CAST-Fish: A New 64-bit Block Cipher", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.4, p. 282,April 2008.

[5] P. Karthigai Kumar, K. Baskaran , An ASIC implementation of low power and high throughput blowfish crypto algorithm, Sciencedirect, 6 April 2010.

[6] Sushanta Kumar Sahu, Manoranjan Pradhan, FPGA Implementation of RSA Encryption System, International Journal of Computer Applications, April 2011.

Deepak Kumar Dakate: Completed B.E. in Electronics & Communication Engineering. Pursuing M. tech in digital communication from Gyan Ganga College Of Technology, Jabalpur (M.P.). Area of research is communication and cryptography.
.

Pawan Dubey: Completed M.E. in Microwave Engineering from JEC Jabalpur. Working as an Asst. Professor at Gyan Ganga College Of Technology ,Jabalpur(M.P.).Area of research is Biometric Recognition, Antenna and Communication.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)