ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 4, June 2012

Performance Comparison of Symmetric Data Encryption Techniques

Deepak Kumar Dakate, Pawan Dubey

***Abstract*- In present scenario various data encryption algorithms are available for data security which has always been important in all aspects of life. Data may contain confidential form of information that one want to secure from any third party access. As we are having number of cryptographic algorithm so sometimes it can create little bit confusion to select best one. This paper provides a view to choose the best available one on the basis of their performance parameter. 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.**

***Index Terms*— Blowfish Encryption, RTL, S BOX, VHDL.**

I. INTRODUCTION

Blowfish Encryption Algorithm:

If the world is to have a secure, unpatented, and freely-available encryption algorithm by the turn of the century, we need to develop several candidate encryption algorithms now. These algorithms can then be subjected to years of public scrutiny and cryptanalysis. Then, the hope is that one or more candidate algorithms will survive this process, and can eventually become a new standard.

Blowfish, a new secret-key block cipher, is proposed. It is a Feistel network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. Blowfish is 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.[1]

Figure given below shows the symmetric encryption process with the application of public key.

***Manuscript received May, 2012*.**

***Deepak Kumar Dakate**, Electronics And Communication, RGPV,Bhopal* Gyan Ganga College of Technology, Jabalpur (M.P.) *(e-mail:* deepakdakate@gmail.com*). Jabalpur, India.*

***Pawan Dubey**, Master of Engineering,JEC Jabalpur.* Gyan Ganga College of Technology, Jabalpur (M.P.) *(e-mail:* pawan_dubey54@yahoo.com*). Jabalpur, India*

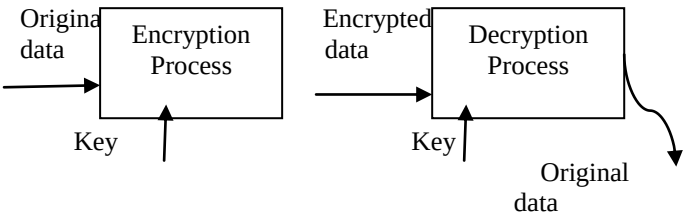


Fig1: Symmetric Encryption/Decryption Process of Blowfish Algorithm

II. HARDWARE IMPLEMENTATION USING VHDL

VHDL (**V**ery High Speed Integrated Circuit **H**ardware **D**escription **L**anguage) was chosen as a language used to describe the improvement suggested to algorithm stated above. VHDL has many features appropriate for describing the behaviour of electronic components ranging from simple logic gates to complete microprocessors and custom chips. Features of VHDL allow electrical aspects of circuit behaviour (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 behavioural) 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.[3]

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.

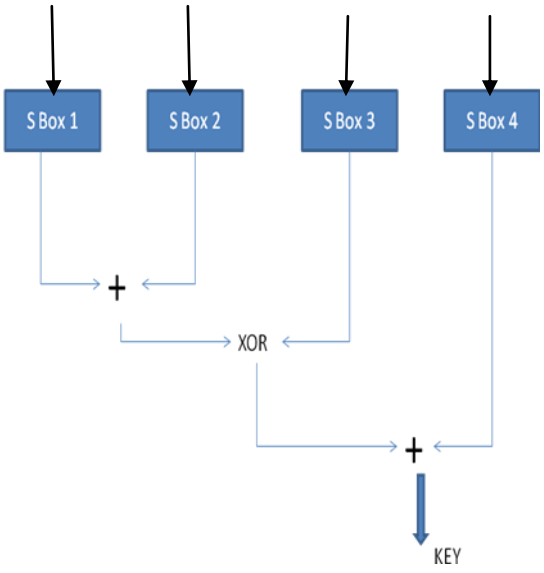


Fig2: Key Generation using Fiestel Network for Blowfish Encryption

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.

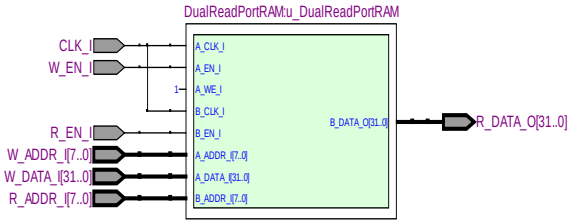


Fig3: RTL View of Single S BOX after Software Simulation.

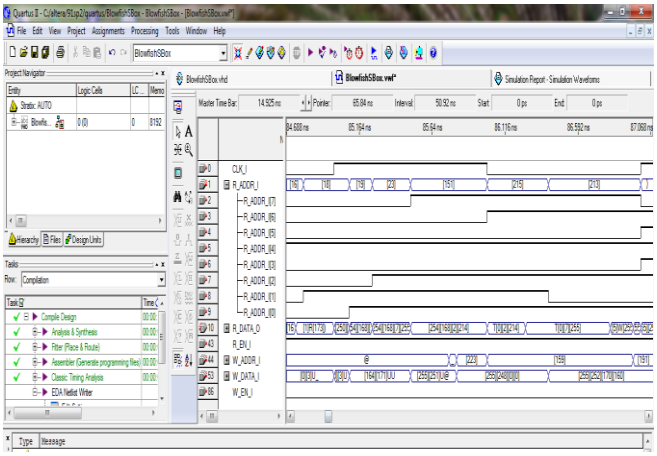
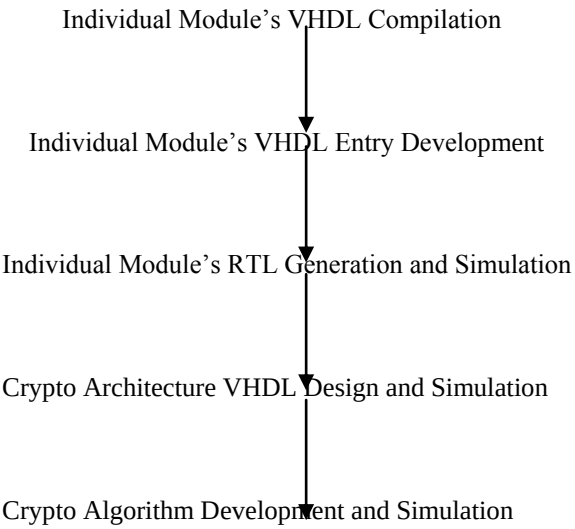


Fig4: Waveform Screenshot of Software Simulation

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.

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



Steps for Encryption Design.[5]

V.POWER PERFORMANCE ANALYSIS

In variable key size Blowfish algorithm the power requirement can be analyzed and compared with other algorithms by varying the key size under certain limit for same logic to generate the same condition that other algorithm follows in terms of key size.

Table 1: Power Analysis For different Key Size.[4][6]

S. No.	Algorithms	Key Size	Power Consumption(mW)
1	BLOWFISH	128	29.86
2	AES	128	2000
3	IDEA	128	58
4	Rijndael	128	82

Power analysis for128 bits key size Blowfish encryption can be compared with other symmetric algorithm which also use 128 bits key size.

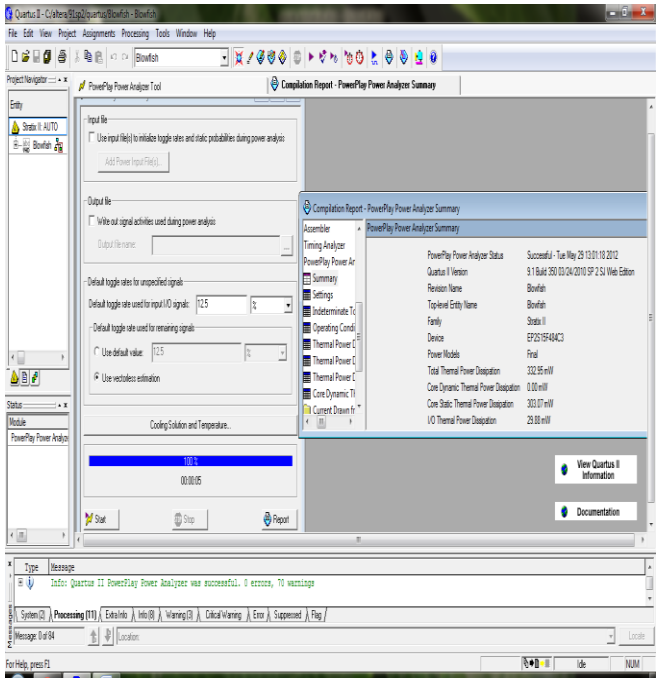


Fig5:Software Screenshot of Poer Analysis.

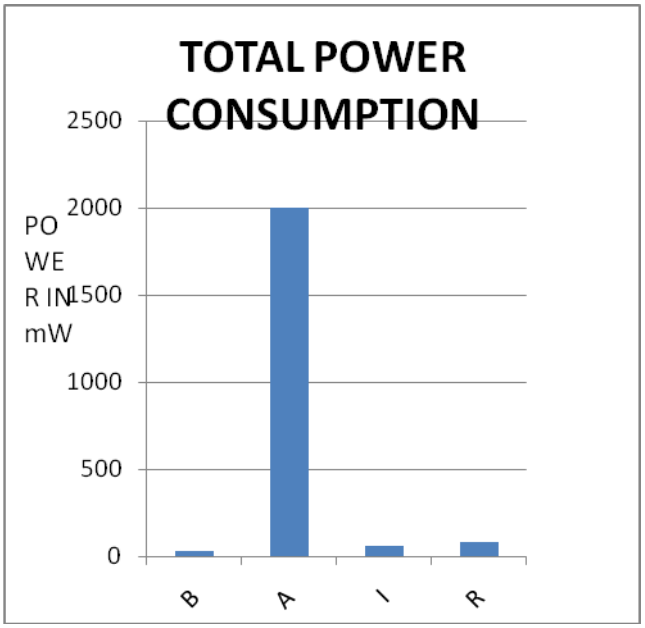


Fig6: Power comparison chart of Blowfish Algorithm(B) with AES(A),IDEA(I) and Rijndael (R)Algorithm.

Figure6 demonstrate the power comparison analysis of Blowfish Algorithm, AES,IDEA and Rijndael Algorithm. From figure it is clear that blowfish consumes negligible amount of power as compared to other algorithm. Among of these AES consumes most amount of power. IDEA And Rijndael consumes more power than blowfish but less than AES.

VI.TIMING ANALYSIS

Table2: Speed comparison Analysis of Blowfish Algorithm with AES,IDEA and Rijndael Algorithm

S. No.	Algorithms	Key Size	Speed (MB/Sec)
1	Blowfish	128	64.386
2	Rijndael	128	61.010
3	Rijndael	192	53.145
4	Rijndael	256	48.229
5	DES	128	21.340

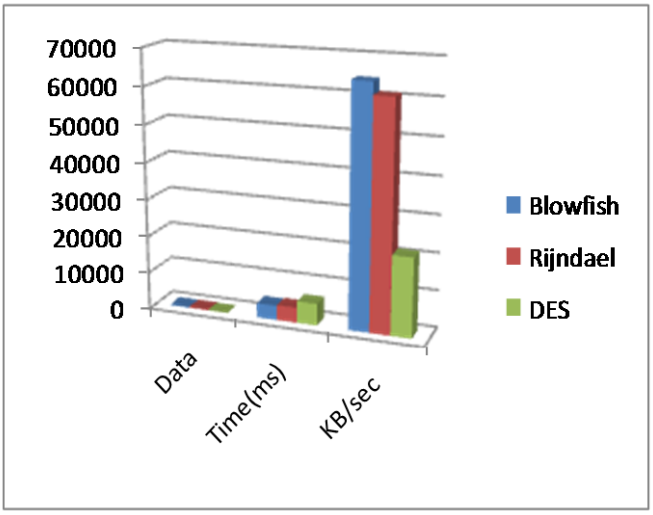


Fig7: Timing Optimization of Blowfish, Rijndael and DES

VII. 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 which is also very less as compared to other shown algorithms. The result also shows superiority of blowfish algorithm over other algorithms on timing constraint.

I. ACKNOWLEDGMENT

II.

Author thanks Mr. Avinash Gaur for his valuable guidance for this paper. Author is very thankful to his colleague for giving time to time advice for different section of paper.

III. 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]NIKOS SKLAVOS, ALEXANDROS PAPAKONSTANTINOU, SPYROS THEOHARIS and ODYSSEAS KOUFOPAVLOU, Low-power Implementation of an Encryption/DecryptionSystem with Asynchronous Techniques, VLSI Design, 2002 Vol. 15

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

[6] M. STRACHACKI and S. SZCZEPAŃSKI, Power equalization of AES FPG Aimplementation, bulletin of the polish academy of sciences technical sciences, Vol. 58, No. 1, 2010

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