IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 5, May 2017

An Approach for High Speed Data Cryptography Technique of Blowfish Algorithm using VHDL

Chanchal D. Pande[1], Prof. S. S. Mungona[2]

Department of Electronics & Telecommunication Engineering, SGBAU University, Gangotri Colony, Tapovan, Amravati, Maharashtra, India[1]

Department of Electronics & Telecommunication , SGBAU University, In front of Nemani Godown, Badnera Road, Amravati, Maharashtra, India[2]

Abstract: Nowadays, higher demand and greater awareness on security problems lead to the study of more secure, high performance, reliable and flexible systems. One method for secure transfer of data is cryptographic method. Cryptography is used to encode the information to keep the information from being hacked by the other party. To meet these demands the implementation of the Blowfish algorithm in the commercial FPGA has been chosen to present the high performance of such FPGA based reconfigurable systems. In this project, we have analyse how such system can be used to enhance the speed of cryptographic computation. By using this FPGA design, the Blowfish computation can be increased in speed. In this project, we have used pipeline structure to enhance speed and also Xilinx software is used for the synthesis purpose. The achieved results lead to the general conclusion that the use of an FPGA coprocessor is ideally suited for the execution of cryptographic algorithms regarding execution time and flexible usage. The performance is analysed in terms of its architecture, throughput, and power consumption.

Keywords: Blowfish algorithm, FPGA processor, VHDL, Modelsim, Xilinx.

I. INTRODUCTION

1.1 Problem Definition

Security has always been a great concern whenever there is communication between sender and receiver. There are various types of attacks mainly Passive attacks and Active attacks. Passive attacks are further divided as Release of message contents and Traffic attacks. Active attacks have types : Masquerade, Denial of service, alterations and Replay Attacks. To overcome the issues of security, many cryptographic algorithms are used like: AES, DES, Triple DES, Blowfish, etc. The objective of this paper is to enhance and evaluate the Blowfish algorithm on the basis of different parameters like encryption quality, speed and throughput. The 'f' function is modified by mixing the XOR and addition operation used in the original algorithm. To meet these demands Blowfish algorithm is implemented using FPGA based reconfigurable systems.

1.2 Motivation

Basically there are two encryption algorithms: symmetric key and asymmetric key encryption algorithm. Symmetric key encryption algorithm is encrypted using the same key for encryption and decryption. While the asymmetric encryption algorithm uses different keys for encryption and decryption. Symmetric key algorithms are less computationally intensive as compared to asymmetric key algorithms. And in practice, asymmetric key algorithms are much slower as compared to the symmetric key algorithms.

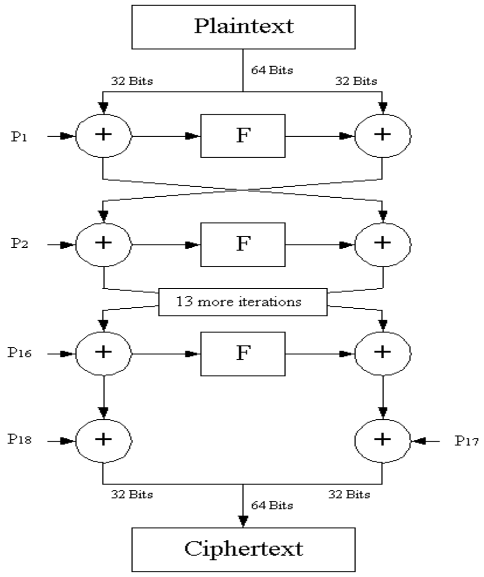
II. PROPOSED WORK

2.1 Blowfish Algorithm

The Blowfish algorithm was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Blowfish is a variable-length key, 64-bit block cipher. The algorithm consists of two parts: a key-expansion part and a data- encryption part. Key expansion converts a key of at most 448 bits into several arrays of4168 bytes. Data encryption occurs via a 16-round Feistel network. Each round consists of a key dependent permutation and data-dependent substitution. All operations are XORs and added on 32-bit words. Blowfish is a 16 rounds Feistal Structure. A Feistel network is a general method of transforming any function (usually called an F function) into a permutation. Every round is made up of a key and data dependent substitution and a key-dependent permutation. All operations are additions on 32-bit words and XOR. The only additional operations, for every round are performed in the following way: 1. Split each block into halves 2. Right half becomes new left half 3. The right half is made when XOR is done on the left half and the result we get after applying 'f' to the right half and the key. 4.

DOI10.17148/IARJSET.2017.4531

The rounds which are prior can be obtained even if the function ‘f’ is not turned upside down.



2.1 Fig Flowchart of blowfish Algorithm

2.2 Function "F" of Blowfish Algorithm

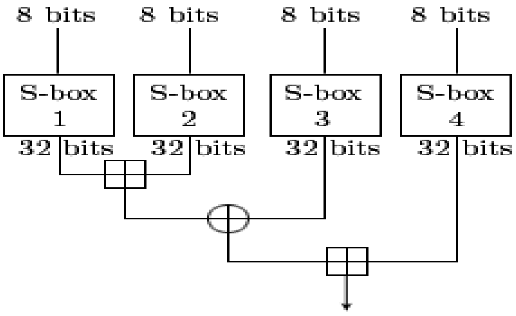


Fig 2.2 Working of Function "F"

Figure 2.2 shows a graphical representation of function F, The function divides a 32 bit input into four bytes and uses those as indices into an Sarray. The lookup results are then added and XORed together to produce the output. As previously mentioned blowfish is a symmetric algorithm and therefore employs the same technique to decrypt a message. The only difference being the output is in plaintext. The Parray and Sarray values used by Blowfish are precomputed based on the user's key. In effect, the user's key is transformed into the Parray and Sarray; the key itself may be discarded after the transformation. The Parray and Sarray need not be recomputed, but must remain secret.

2.3 FPGA

Field Programmable Gate Arrays can be programmed or configured by the user or designer after manufacturing and during implementation. Their structure is similar to that of a gate-array or an ASIC. Thus, they are used to rapidly prototype ASICs, or as a substitute for places where an ASIC will eventually be used. The programming of the FPGA is done using a source code using a HDL.

2.4 VHDL

VHDL is an acronym for VHSlC Hardware Description Language (VHSIC is an acronym for Very High Speed Integrated Circuits). It is a hardware description language that can be used to model a digital system at many levels of abstraction ranging from the algorithmic level to the gate level. The complexity of the digital system being modeled could vary from that of a simple gate to a complete digital electronic system, or anything in between.

2.5 TEST BENCH

A test bench is HDL code that allows to provide a documented, repeatable set of stimuli that is portable across different simulators. A test bench can be as simple as a file with clock and input data or a more complicated file that includes error checking, file input and output, and conditional testing

DOI10.17148/IARJSET.2017.4531

III. SYSTEM IMPLEMENTATION

3.1 System Architecture

The system architecture consist of various blocks like P array, S box, PiROM and blowfish cipher. Initially data is given to P array and this data is encrypted by using key. PiROM is used as a storage purpose and S boxes performs substitution operation. All this data is combined and given to Blowfish cipher and finally output data is taken from output port of Blowfish cipher.

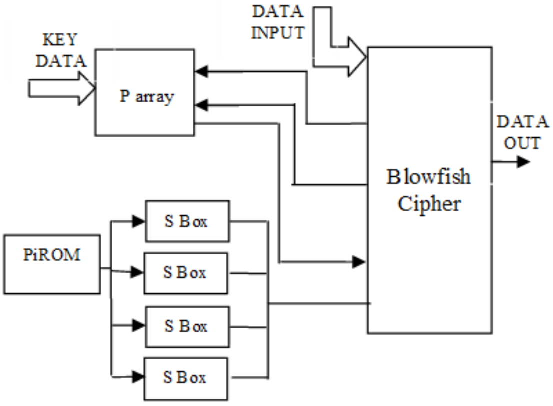


Fig 3.1 System Architecture

3.2 Pipeline Structure

In computing, a pipeline is a set of data processing elements connected in series, where the output of one element is the input of the next one. The elements of a pipeline are often executed in parallel fashion, in that case, some amount of buffer storage is often inserted between elements. Pipelining increases instruction throughput by performing multiple operations at the same time (concurrently), but does not reduce instruction latency (the time to complete a single instruction from start to finish) as it still must go through all steps. Indeed, it may increase latency due to additional overhead from breaking the computation into separate steps. Pipelining thus increases throughput at the cost of latency, and is frequently used in CPUs, but avoided in real time systems, where latency is hard constrain.

3.3 Project Design Flowchart

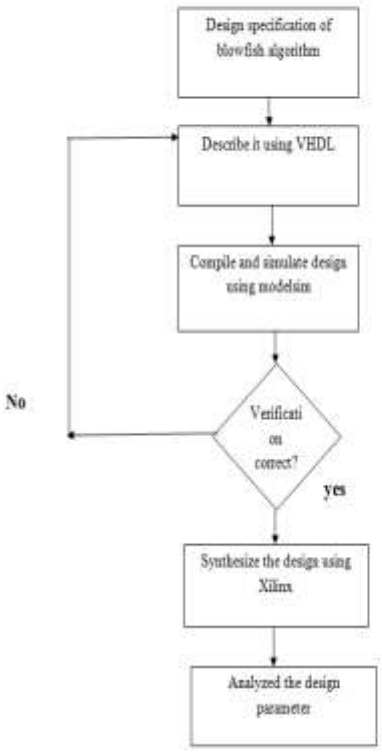

Design specification of blowfish algorithm
Describe it using VHDL
Compile and simulate design using modelsim
No
Verificati on correct?
yes
Synthesize the design using Xilinx
Analyzed the design parameter

Fig 3.2 Project Design Flowchart

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

- Blowfish is described using VHDL
- Simulation is achieved using modelsim
- This verification checked and if it is correct then it is further synthesized using Xilinx
- If verification is not correct then code is again given back to VHDL and then again it is compiled
- Finally design parameters are analyzed

IV. RESULT AND DISCUSSION

4.1 Simulation

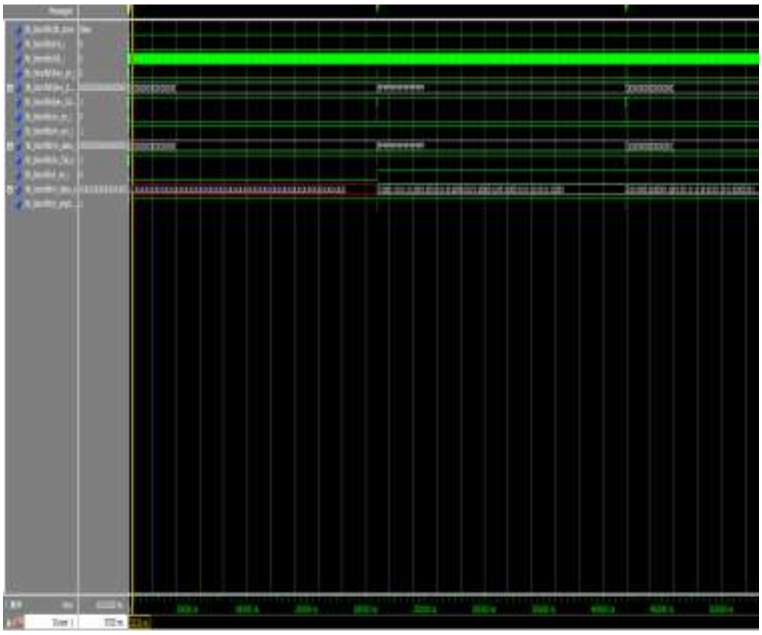
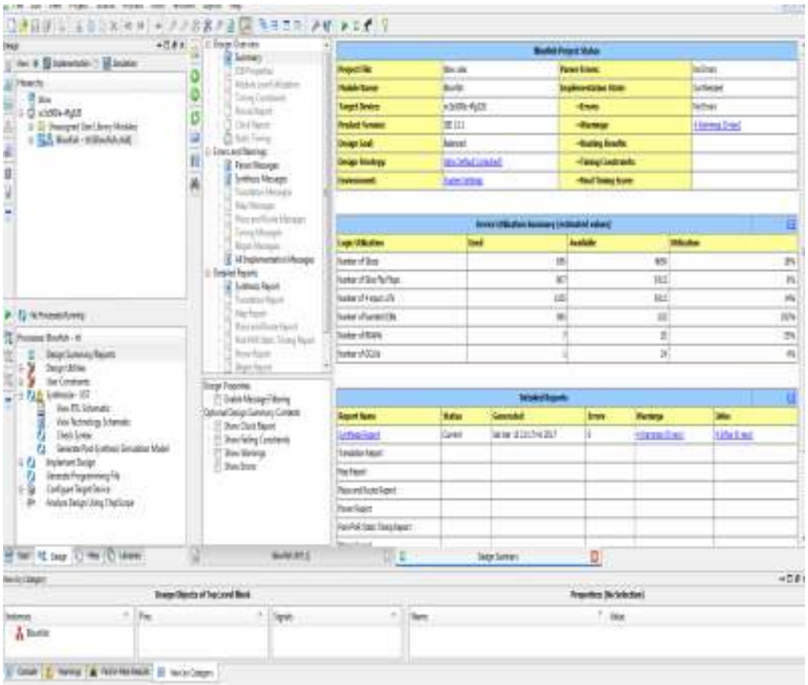


Fig 4.1 Simulation

4.2 Synthesis

4.2.1. Design Summary



Logic Utilization	Used	Available	Utilization
Number of Slices	[illegible]	[illegible]	[illegible]
Number of Slice Flip Flops	[illegible]	[illegible]	[illegible]
Number of 4 input LUTs	[illegible]	[illegible]	[illegible]
Number of bonded IOBs	[illegible]	[illegible]	[illegible]
Number of BRAMs	[illegible]	[illegible]	[illegible]
Number of GCLKs	[illegible]	[illegible]	[illegible]

Fig 4.2 Design Summary

DOI10.17148/IARJSET.2017.4531

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

4.2.2 RTL Schematic

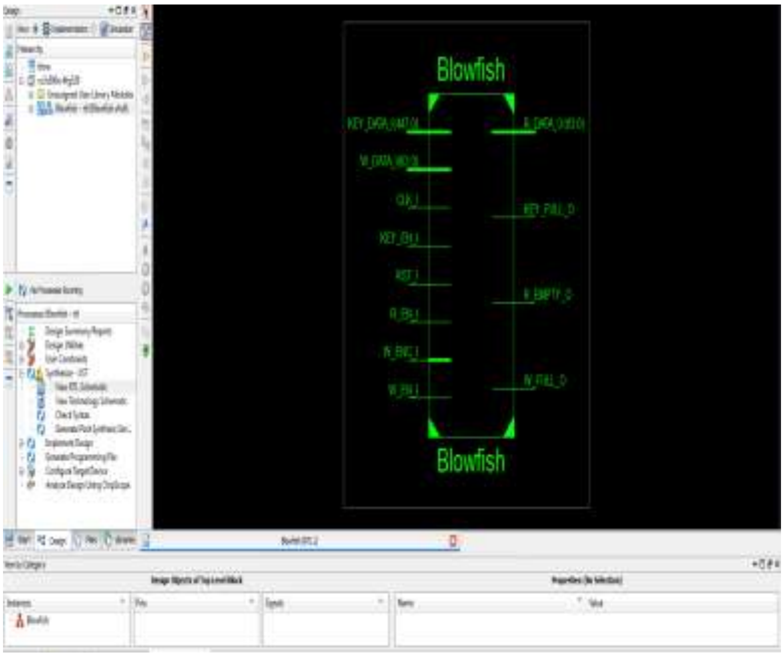


Fig 4.3 RTL Schimetic

V. CALCULATIONS

Throughput= (No of bits * Maximum Frequency)/No of clock cycles

Time	14.717ns
Frequency	67.950mhz
LUTs	1335

VI. CONCLUSION

While communicating, there is a high possibility of hacking the information between two or more users. So as to protect the system from various attacks security is important. There are number of ways to protect these attacks. For that, there is a need to learn how to combine the approaches to completely solve these problems. Proposed Framework is one such unique technique compose of various defence mechanism. So by using blowfish algorithm and VHDL, high level of information security is achieved. In this project we have encrypted the text data. So in future, along with text data, image, video as well as audio can also be encrypted. To encrypt video, pixel mapping can be used.

REFERENCES

[1] Kurniawan Nur Prasetyo, YudhaPurwanto, Denny Darlis, "An implementation of data encryption for internet of things using Blowfish algorithm based on FPGA", Vol 2, 2014.
[2] Amaal A. Abd El-Sadek, Talaat A. El-Garf, Mohammed M.Fouad, "Speech Encryption Applying a Modified Blowfish Algorithm", October 2014.
[3] Metaliya Viral, Deepak Kumar Jain, Sardhara Ravin, "A Real Time Approach for Secure Text Transmission Using Video Cryptography", Vol 4, 2014.
[4] Viney Pal Bansal,Sandeep Singh, "A Hybrid Data Encryption Technique using RSA and Blowfish for Cloud Computing on FPGAs", December 2015.
[5] Sudeshna Bora, Pritam Sen and Chittaranjan Pradhan, "Novel Color Image Encryption Technique using Blowfish and Cross Chaos Map", 2015.
[6] Rafidah Ahmad, AsrulnizamAbd. Manaf, "Development of an Improved Power-Throughput Blowfish Algorithm on FPGA",Vol 12, 06 March 2016.
[7] Nusrat Jahan Oishi, Arafin Mahamud, Asaduzzaman, "Enhancing Wi-Fi Security Using a Hybrid Algorithm of Blowfish and RC6", 2016.
[8] Kapil Earanky, Haytham Elmilig, Musfiq Rahman, "Cryptographic GPU-Acceleration of Blowfish Algorithm".
[9] Vaibhav Poonia, Dr.Narendra Singh Yadav, "Analysis of modified Blowfish Algorithm in different cases with various parameters", January 2015.
[10] Neha Khatri, Prof. V. K Kshirsagar, "Blowfish Algorithm", 2008.
[11] H. Singpiel, H. Simmler, A. Kugel, "Implementation of Cryptographic Applications on the Reconfigurable FPGA Coprocessor microEnable", 2000.
[12] Tingyuan Nie; Chuanwang Song; Xulong Zhi, "Performance Evaluation of DES and Blowfish Algorithms," International Conference on Biomedical Engineering and Computer Science, vol., no. 2, pp.1-4, 23-25 April 2010.
[13] Nentawe Y. Goshwe, “Data encryption and decryption using RSA algorithm in a network environment”, International Journal of Computer Science and Network Security, vol..13 No.7, pp. 9-13, 2013.
[14] Minni, R.; Sultania, K.; Mishra, S.; Vincent, D.R., "An algorithm to enhance security in RSA," International Conference on Computing, Communications and Networking Technologies, vol., no. 4, pp.1-4, 4-6 July 2013

DOI10.17148/IARJSET.2017.4531