International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 12 113 – 116

High Speed Data Cryptography Technique of Blowfish Algorithm using VHDL

Chanchal D. Pande
Electronics & Telecommunication Engineering, SGBAU,
Gangotri Colony near Tapovan Gate,
Amravati, Maharashtra, India.
chanchalpande8@gmail.com

Prof. S. S. Mungona
Electronics & Telecommunication , SGBAU,
In front of Nemani Godown,
Opposite Nemani Godown, Badnera Road,
Amravati, Maharashtra, India
mungona@rediffmail.com

***Abstract*—**Nowadays, information security is more important issue for reliable data transfer. A cryptographic method is widely used to ensure the security of data. To keep the information from being hacked by the other party, data is encoded by using this method. To meet these requirements the implementation of the Blowfish algorithm in the commercial FPGA has can be used to obtain high performance of such FPGA based reconfigurable systems. This paper presents, how such a system can be used to enhance the speed of cryptographic computation. By using FPGA design, the Blowfish computation can be increased in speed. In this, Xilinx software is used for the analysis purpose. The results will 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 analyzed in terms of its architecture, speed, throughput, and encryption time.

Keywords- *Blowfish algorithm, FPGA processor, VHDL design.*

*****

I. INTRODUCTION

Cryptography is a way of protecting the information by transforming it into an unreadable format known as cipher text. Plain text is converted into cipher text using encryption key. Only the person who possess the secret key can decipher the message into the original form. The information looks like hidden inside the image or the text file. The encryption key is used to encrypt the data. This encrypted information is then transmitted to the particular receiver. At the receiver end, cipher text is converted back into plain text using description key. Receiver extracts the original information from the image or a text with the help of a public key provided by the transmitter. So even if any unwanted person gets the data with information content hidden in it, it cannot be extracted without appropriate public key.

There are two types of encryption algorithms: symmetric key encryption algorithm and asymmetric key encryption algorithm. Symmetric key encryption algorithm or private key encryption uses same key for encryption and decryption. Security. While the asymmetric encryption algorithm or public key encryption uses two different keys for encryption and decryption. Blowfish algorithm is symmetric encryption algorithm. Blowfish algorithm has simple structure and it can perform encryption and decryption process quickly. There are two ways to implement the cryptographic algorithms via software or hardware implementation. One type of hardware implementation is using FPGA. FPGA or Field Programmable Gate Arrays can be programmed or configured by the user or designer after manufacturing and during implementation. Hence they are also known as On-Site programmable. Unlike a Programmable Array Logic (PAL) or other programmable device, 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 Hardware Description Language (HDL) to specify how the chip should work. VHDL language is used for implementation on FPGA. FPGA is widely used because of several reasons, it is cheap, easy to implement, reprogrammable, has high speed and good level of security.

II. LITERATURE REVIEW

Various authors made a research on the implementation and modifications of blowfish algorithm for efficient results.

1] Kurniawan Nur Prasetyo, Yudha Purwanto, Denny Darlis 2014

This paper presents blowfish algorithm is implemented on FPGA using VHDL programming language. The testing showed that blowfish algorithm gave a good performance when implemented in FPGA. This research also presents the performance of blowfish algorithm with total time taken for

encryption. The result shows that reducing the total encryption time, give greater throughput and not affect avalanche effect significantly [1].

2] Amaal A. Abd El-Sadek, Talaat A. El-Garf, Mohammed M. Fouad 2014

This paper presents the high quality speech coding algorithm which has been standardized by ITU-T with low bit rate. This algorithm is based on a conjugate structure algebraic coding technique. This paper proposes a new method for generating S-boxes and P-arrays. This new generating method leads to a reduction in time complexity of generating S-boxes and P-arrays. The results showed that the modified design of the algorithm offers the same level of security as the original blowfish cipher with a less complexity [2].

3] Metaliya Viral, Deepak Kumar Jain, Sardhara Ravin 2014

This paper uses video cryptography is used for secure transmission of data. It uses pixel mapping for the encryption of the images which are the basic building blocks of any video file. Any video is a combination of different frames and all the frames has fixed frame rate. The video is distributed into the photo frames using a matlab code then all the frames are sequentially stored. Each such frame contains a combination of red, blue and green layers. After the completion of the pixel mapping, all the images are placed in a sequential manner and then all the frames are cascaded for generation of the original video file with encryption. This new video is almost same as that of original video with no changes visible to the naked eye [3].

4] Viney Pal Bansal, Sandeep Singh 2015

This paper uses hybrid technique which is implemented using VHDL coding. The Xilinx ISE 14.1 is used for synthesis purpose. It uses hybrid RSA and blowfish encryption technique which is implemented by VHDL. This hybrid technique has both symmetric and asymmetric properties. Thus, the algorithm provides better security for cloud computing. Also hybrid algorithm is successfully implemented by using VHDL. [4]

. 5] Sudeshna Bora, Pritam Sen, Chittaranjan Pradhan 2015

This paper uses an image encryption scheme used to protect different types of images. In this algorithm, the blowfish and cross chaos are combined to form double encryption algorithm. The designed scheme secures the color image. For decryption, original images are obtained using the same key and by applying the same cross chaos parameters that were used during the time of encryption. Simulation and analysis results tells that the Blowfish algorithm is able to protect different types of images with a high security [5].

6] Rafidah Ahmad, Asrulnizam Abd. Manaf 2016

This paper presents a development of an improved power throughput using blowfish algorithm based on field programmable gate array (FPGA).The performance is analysed in terms of its speed, throughput, and power. Results show that the proposed Blowfish reduces time and increases throughput at low power consumption [6].

7] Nusrat Jahan Oishi, Md.Arafin Mahamud, Asaduzzaman 2016

This paper presents, a hybrid form algorithm of Blowfish and Rivest Cipher 6 (RC6) which is used which solves the security problems of blowfish and maintains the efficiency of blowfish. Thus, it is able to use in place of AES. The usage of one S-Box by overlapping process eliminates the collision attack of blowfish algorithm. Sub key generation process removes the Brute Force attack. It enhances the performance of Blowfish algorithm by using a function of RC6 . The proposed algorithm takes less encryption-decryption time and thus increases speeed of system [7].

8] Kapil Earanky, Haytham Elmiligi, Musfiq Rahman

This paper present a CUDA (Compute Unified Device Architecture) implementation of the blowfish algorithm. It has been designed to make use of the unified memory model. Result tells that the unified implementation of the blowfish algorithm performs better than an efficient CPU implementation and performs better than a non-unified CUDA implementation of the algorithm. Using (CUDA) design, the paper describes the implementation and performance enhancement of the blowfish block cipher algorithm [8].

III. PROPOSED WORK

Blowfish algorithm was designed in 1993 by Bruce Schneier as a fast, reliable encryption algorithm. Blowfish is a variable-length key, 64-bit block cipher. The algorithm consists of two parts: a key-expansion part and data- encryption part. Key expansion converts a key of at most 448 bits into several arrays of 4168 bytes. Data encryption occurs via a 16-round Feistel network. Where each round consists of a key dependent permutation and data-dependent substitution. All operations are XORs and then added on 32-bit words. A Feistel network is a general method of transforming any function (usually called an F function) into a permutation. Every round consist of a key and data dependent substitution and a key dependent permutation. The algorithm works as follows:

 ISSN: 2321-8169
113 – 116

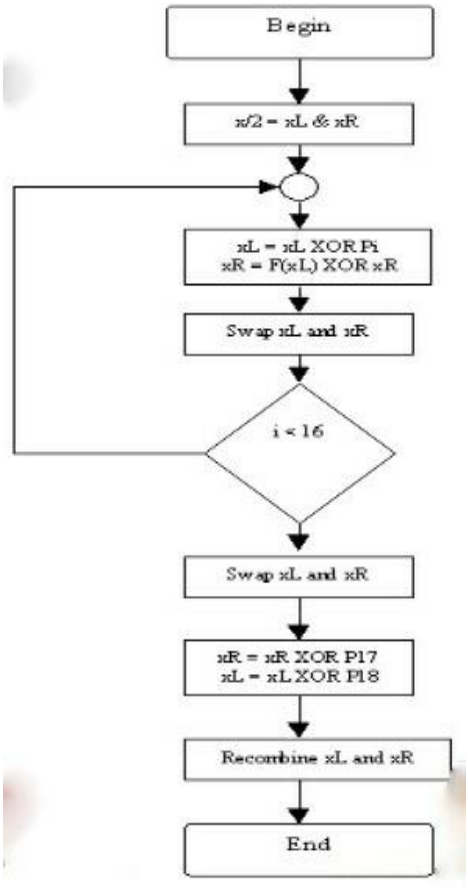

Fig 1.2 Flow chart of Blowfish algorithm

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.

Encryption:-

Blowfish has 16 rounds.

The input is a 64-bit data element, x.

Divide x into two 32-bit halves: xL, xR.

Then, for i = 1 to 16:

xL = xL XOR Pi

xR = F(xL) XOR xR

Swap xL and xR

After the sixteenth round, swap xL and xR again to undo the last swap.

Then, xR = xR XOR P17 and xL = xL XOR P18.

Finally, recombine xL and xR to get the ciphertext.

Description

Initially the input is given to the MATLAB simulink. The data can be a text or image. If the data is image then it is converted from 1D to 2D by means of matlab. This binary sequence is then given to FPGA which do the programming using VHDL in Xilinx. Then this data is again converted back into original form and at the end output is taken.

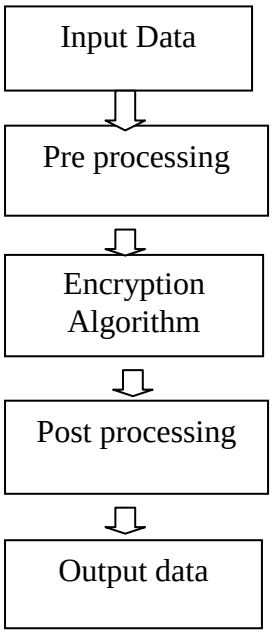

Fig 1.4 Block Diagram of Internal Component

Pre-processing is used because FPGA takes the input in binary form only. In this, the input image is converted from RGB to Gray and then by using A to D convertor it is converted to binary form. This binary data is given to FPGA. After applying blowfish algorithm, the data is transmitted for Post processing where the binary image is converted from Gray to RGB form. Finally, the encrypted image is taken at the output. For coding purpose VHDL is used. The VHDL Hardware Description Language is a formal notation intended for use in all phases of the creation of electronic systems. Because it is both machine readable and human readable, it supports verification, synthesis, and testing of hardware designs. The digital system may be a simple logic gate or it may be a complete electronic system.

IV. CONCLUSIONS

Hacking attacks are complex which causes serious problem on Internet. There are numerous ways to protect these attacks so 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 two different defense mechanism. So by using blowfish algorithm, information security can be achieved to large extent.

As the research is going on, new features will be added that will only increase their security and speed.

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] H. Singpiel, H. Simmler, A. Kugel, "Implementation of Cryptographic Applications on the Reconfigurable FPGA Coprocessor microEnable", 2000.