ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 1, March 2018

6th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '18)

13th-14th March 2018

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

FPGA Implementation of Cryptography Using Blowfish Algorithm

Kaviyanandhini.M[1], Keerthana.S[2], Maheshwari.V[3], Nidharshana.S[4] and Nagaraju.N[5]

UG Scholar, Department of ECE, Adhiyamaan College of Engineering, Hosur, TN, India [1,2,3,4]

Associate Professor, Department of ECE, Adhiyamaan College of Engineering, Hosur, TN, India[5]

ABSTRACT: Cryptography is the one of the main categories of computer security that converts information from its normal form into an unreadable form. In this project, a Blowfish algorithm for information security is a symmetric block cipher that provides good encryption and decryption rate in software. It is a 16 round feistel cipher and uses large key dependent S-boxes. It has a 64 bit block size and a variable key length from 32 bits upto 448 bits. This is done for network security and defence applications.The simulation result is going to be analyzed by Xilinx ISE software using the VHDL language.

KEYWORDS*:* Xilinx ,Cipher, Plaintext, Blowfish, Feistel block.

I. INTRODUCTION

Security plays an important role to store information and transmit it across the undefined networks with secure manner. Hence, the secure communication is the basic requirement of every transaction over networks [1-3]. Cryptography is an essential component for secure communication and transmission of information through security services like confidentiality, data integrity, access control, authentication and non-repudiation.

It provides a way to protect sensitive information by transferring it into unintelligible and only the authorized receiver can be able to access this information by converting into the original text.

The process to convert the plaintext into ciphertext with the key is called encryption process and to reverse the process of encryption is called decryption process.

The design of cryptographic algorithms is secure and efficient, low cost, require small memory footprint, easy to implement and utilized on multiple platforms. The vast range of applications is developed to secure cryptographic algorithms using different mathematical process [2]. It is quite difficult to develop fully secure encryption algorithm due to the challenges from cryptanalysts who continuously trying to access any available cryptographic systems[4] .The right selection of algorithms is important to achieve high-security requirements which protect the cryptographic components to cryptanalysis.

II. BLOWFISH ALGORITHM

Blowfish is a symmetric block cipher. It has a fixed 64-bit data block size and a variable secret key range from 32 bits to 448 bits. The algorithm consists of two parts: key expansion and data encryption. The key expansion converts a key of at most 448 bits into several subkey arrays totalling 4168 bytes[1].

The data encryption occurs via a 16-round Feistel network. Each round consists of a key-dependent permutation, and a key- and data dependent substitution. All operations are XORs and additions on 32-bit words [2]. The only additional operations are four indexed array data lookups per round.

EXISTING METHOD

As blowfish is a variable length key block cipher, it is most suitable for applications where the key does not often change such as a communications link or an automatic file encryptor . Horst Feistel published an article on Feistel Network in 1973. Most symmetric block ciphers use Feistel Network for their construction.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 1, March 2018

6th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '18)

13th-14th March 2018

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

A Feistel Network is said to be an iterative network which consists of an internal function called as round function. It is a method where the round function (also called as F-function) is transformed into permutation [5]. The Feistel Network working can be summarized as follows:-

- The input data is split into two equal halves.
- The right half of input data becomes the new left half.
- The round function (F-function) is applied to the right half of input data and the key.
- The output of the F-function is then xored with the left half of input data.
- The output from the xor operation is the new right half.
- The new right half and the new left half becomes the Feistel Network output.

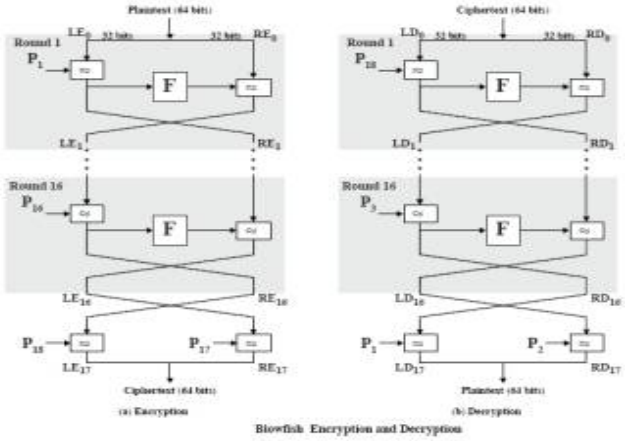

Fig 1: Existing method process

FIESTEL BLOCK

Blowfish uses 4 8x32 S-boxes. The total memory consumed for storing the 4 S-boxes are 4096 bytes and in addition 512 iterations of encryption is required to store the values of S-box [4-5]. An alternative way to reduce the memory and computational time taken by these S-boxes would be to use the substitution bytes and mix columns concept of AES [2].

The S-box in AES is designed such that the correlation between the input and output bits is very low and the mix column helps in mixing the output bytes of the S-box. Since blowfish requires 4 S-boxes, the AES s-box is rotated in cyclical manner to avoid any symmetric patterns between the output bytes of S-box.

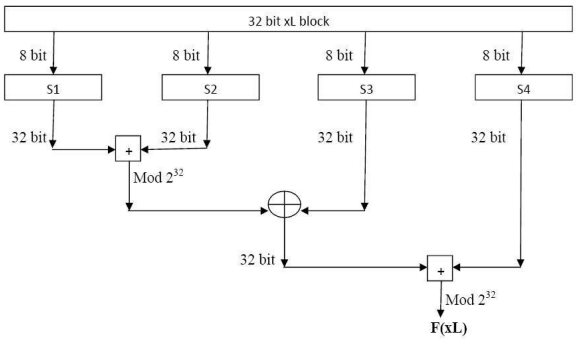

Fig 2: Fiestel block

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 1, March 2018

6th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '18)

13th-14th March 2018

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

It is having a function to iterate 16 times of network. Each round consists of key-dependent permutation and a key and data-dependent substitution. All operations are XORs and additions on 32-bit words[4]. The only additional operations are four indexed array data lookup tables for each round.

ADDERS

In existing method the delay and area realization were made by using ripple carry adder, carry look ahead adder and carry save adders in the fiestel block of thew blowfish algorithm.

EXISTING METHOD DISADVANTAGES

The ripple carry adder used in the feistel block has the following disadvantage:

- Long delay due to the propagation of carry from low to higher order stages.
- The key to speeding up addition is determining carry values sooner.

The Carry look ahead adder disadvantage is that the carry logic block gets very complicated for more than 4-bits[2]. For that reason, CLAs are usually implemented as 4-bit modules and are used in a hierarchical structure to realize adders that have multiples of 4-bits.

The carry save adder has the disadvantage that,
We know the result of the addition at once. We still do not know whether the result of the addition is larger or smaller than a given number(for instance, we do not know whether it is positive or negative).

This latter point is a drawback when using carry-save adders to implement modular multiplication(multiplication followed by division, keeping the remainder only)[3]. If we cannot know whether the intermediate result is greater or less than the modulus, we cannot know whether to subtract the modulus.

PROPOSED METHOD

In the proposed method the ripple carry adder has been replaced by carry select adder for faster performance.

ALGORITHM

Divide x into two 32-bit halves: xL, xR
For i = 1to 32:

- xL = XL XOR Pi
- xR = F(XL) XOR xR
- Swap XL and xR
- Swap XL and xR (Undo the last swap.)
- xR = xR XOR P17
- xL = xL XOR P18

Recombine xL and xR

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 1, March 2018

6th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '18)

13th-14th March 2018

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

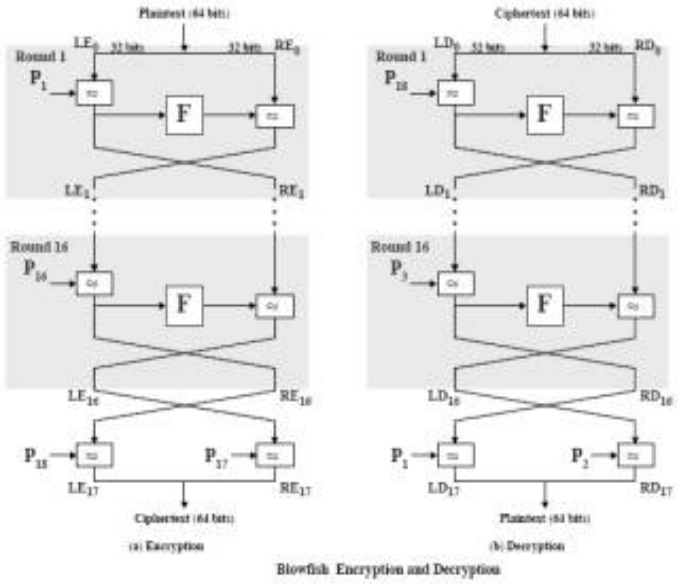

Fig 3: Proposed method with carry select adder in the fiestel block

For decryption, the same process is applied, except that the sub-keys Pi must be supplied in reverse order. The nature of the Fiestel network [1] ensures that every half is swapped for the next round (except, here, for the last two sub-keysP17 and P18).

CARRY-SELECT ADDER

Carry Select Adder (CSA) is known to be the fastest adder among the conventional adder structures. Low-power, area-efficient, and high-performance VLSI systems are increasingly used in portable and mobile devices, multistandard wireless receivers, and biomedical instrumentation [1], [2]. An adder is the main component of an arithmetic unit. A complex digital signal processing (DSP) system involves several adders. An efficient adder design essentially improves the performance of a complex DSP system. A ripple carry adder (RCA) uses a simple design, but carry propagation delay (CPD) is the main concern in this adder.

It is used in many data processing units for realizing faster arithmetic operations. In this paper, we present an innovative CSA architecture. It employs a novel incrementer circuit in the interim stages of the CSA. Validation of the proposed design is done through design and implementation of 16, 32 and 64-bit adder circuits. Comparisons with existing conventional fast adder architectures have been made to prove its efficiency. The performance analysis shows that the proposed architecture achieves three fold advantages in terms of delay-power.

The carry-select adder generally consists of two ripple carry adders and a multiplexer. Adding two n-bit numbers with a carry-select adder is done with two adders (therefore two ripple carry adders), in order to perform the calculation twice, one time with the assumption of the carry-in being zero and the other assuming it will be one.

After the two results are calculated, the correct sum, as well as the correct carry-out, is then selected with the multiplexer once the correct carry-in is known.The number of bits in each carry select block can be uniform, or variable. The delay is derived from uniform sizing, where the ideal number of full-adder elements per block is equal to the square root of the number of bits being added, since that will yield an equal number of MUX delays.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 1, March 2018

6th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '18)

13th-14th March 2018

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

ADVANTAGE OF CARRY-SELECT ADDER

The main advantage of CSA is its reduced propagation delay characteristics. This is realized by the use of parallel stages that results from multiple pairs of ripple carry adder. The ripple carry adders generate their interim sum and carry for the CSA structure by considering the carry input to be 0 and 1 respectively.

III. SIMULATION RESULTS

The simulated output of the blowfish algorithm process is shown below

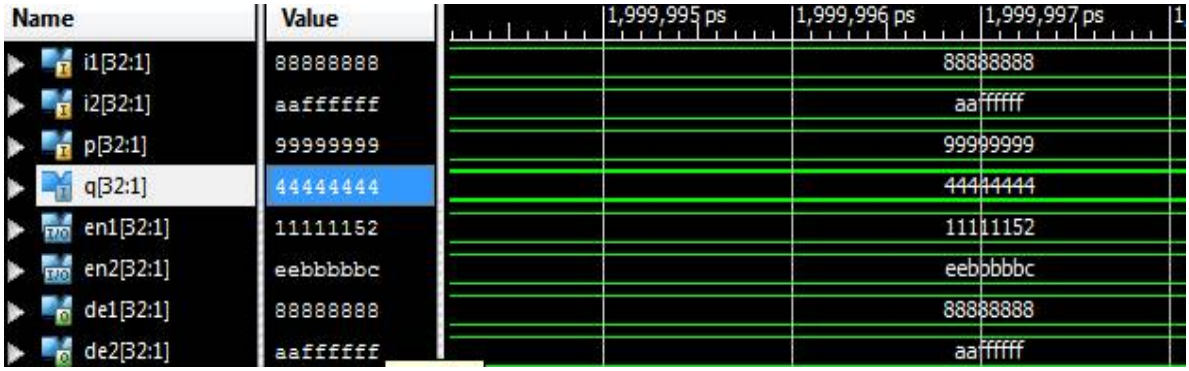

Fig 4: Output of cryptographic process

In the above output the main input is divided into i1 and i2 each of 32 bits. And the two keys p and q are used. The encrypted result is denoted as en1 and en2.And the decrypted result is denoted as de1 and de2

COMPARISON OF EFFICIENCY

Table 1: Comparison of LUTs and delay

	SPARTAN 3		SPARTAN 6		VERTEX 5	
	LUT	DELAY	LUT	DELAY	LUT	DELAY
RIPPLE CARRY ADDER	1033	436.113	1314	251.742	1394	147.049
CARRY SAVE ADDER	1429	503.019	2060	283.069	2179	181.816
CARRY SELECT ADDER	1033	442.182	1285	216.632	1392	149.416

IV. CONCLUSION

The proposed architecture should satisfy the need of high-speed data encryption and can be applied to various devices respectively[2]. In this paper we discussed Blowfish algorithm, it is a variable-length key block cipher. It is suitable for applications where the key do not change often, like a communications link[4]. It is faster than DES. The present simulation result shows that the encryption and decryption is done using blowfish algorithm. Here the algorithm is modified so it provides great security thus no one in between sender and receiver will hack the data.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 1, March 2018

6th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '18)

13th-14th March 2018

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

Blowfish is a 16 pass block encryption algorithm that is never broken.
Blowfish is used frequently because:

- It has been repeatedly tested & found to be secure.
- It is fast due to its taking advantage of built-in instructions on the current microprocessors for basic bit shuffling operations.
- It was placed in the public domains.

REFERENCES

[1] Somayeh Timarchi, Keivan Navi – Improved Modulo 2n +1 Adder Design, International Journal Of Computer and Information Engineering 2:7 2008.
[2] Kurniawan Nur Prasetyo, YudhaPurwanto, Denny Darlis, "An implementation of data encryption for internet of things using Blowfish algorithm based on FPGA", Vol 2, 2014.
[3] T. Nie and T. Zhang "A Study of DES and Blowfish Encryption Algorithm," IEEE TENCON Singapore, pp.1-4, Jan 2009.
[4] Akhil Kaushik, Manoj Barnela, Anant Kumar, "G.Block Encryption standard for transfer of data", IEEE , 978-1-4244-7578-0, 2010
[5]Web site: www.schneier.com/academic/blowfish/
[6] Sushanta Kumar Sahu, Manoranjan Pradhan, FPGA Implementation of RSA Encryption System, International Journal of Computer Applications, April 2011.
[7] B. Schneier, "Applied Cryptography," 2nd ed. New York: , JohnWiley & Sons, Inc., 1996.
[8] B.Schneier.The Blowfish Encryption Algo-rithm. Retrieved 12:04:58, July 27, 2007 from http://www.schneier.com/blowfish.html
[9] B. Schneier, "Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish)," *Fast Software Encryption: Second International Workshop, Leuven, Belgium, December 1994, Proceedings*, Springer- Verlag, 1994, pp. 191-204.
[10] "Design of the Multi-channel Ultrasonic Signal Acquisition and DenoisingBased on FPGA," Liu Jun, Miao Changyun, BaiHua and Yang Yanli, Seventh International Conference on Measuring Technology and Mechatronics Automation, 2015.