Design And Performance Analysis of High-Speed Blowfish Cryptosystem

G Rajesh Kumar, ECE Department, CMR College of Engineering & Technology, Hyderabad, Telangana, India.
Mohiul Islam, ECE Department, CMR College of Engineering & Technology, Hyderabad, Telangana, India.
G. Prasanna Kumar, ECE Department, Vishnu Institute of Technology, Bhimavaram, A.P. India.

Article Info
Volume 82
Page Number: 3181 - 3186
Publication Issue:
January-February 2020

Article History

Article Received: *14 March 2019*
Revised: *27 May 2019*
Accepted: *16 October 2019*
Publication: *19 January 2020*

Abstract

In the era of information on cloud, the information security plays a critical role. There are so many security schemes available. All the available security schemes developed by many folds encoding of original data. Because of these complex many fold security steps, all these algorithms taking long time to compute the cipher text. Blow fish algorithm is a popular encryption scheme. This algorithm involves many complex stages. To compute these complex stages, software program may take long time. There by many other factors like power consumption and throughput also effects. To avoid these difficulties, a high-speed crypto algorithm based on Blowfish security scheme is developed. Hardware implementation of the proposed algorithm may be useful in high-speed communication systems. Entire system is described using Verilog HDL and is implemented using Spartan 3E FPGA.

Keywords: *Blowfish, Cipher text, Data Security, Decryption, Encryption.*

I. INTRODUCTION

Privacy and security are critical issues in wireless communication systems. Especially while working with Internet of Things (IoT) and Cloud computing. Data security is gaining importance in these days. Due to high speed communication and low data transfer costs, most of the data transfer applications and users are preferring multimedia communications. When the multimedia data communication increases, the fraudulent communication also increases in parallel. To secure the data communication, a high-speed and reliable security system is needed. Blowfish algorithm is a reliable technique which was used in many data communication techniques. But the complexity of the algorithm is very high. Because of the high complexity, the execution time of the algorithm is also high.

A high-speed and less complex security system is very much needed in present day data communication industry. Utilization of FPGA for execution of cryptographic calculations is effective and helpful procedure. FPGA is modest, simple to actualize, effectively reprogrammable, exceptionally fast what's more, abnormal state of security. Generally, for FPGA sheets, VHDL is normally utilized. It utilizes abnormal state demonstrating for them develops. The idea of bundles in VHDL, library the board and separate gathering makes it solid for higher level framework.

Cryptography for Data security is an exceptionally incredible technique for assurance of information From being stolen. Cryptography is a approach to encode the statistics to shield the information from being hacked by using the opportunity celebration. Cryptography has two strategies, symmetric, and asymmetric cryptographic algorithms. In Symmetric cryptography, same secret is applied and percentage for every Encryption and Decryption. Where as in uneven cryptography, exclusive keys are carried out for Encryption and Decryption. Symmetric cryptography is essential in shape and short. Blowfish is a case of Symmetric cryptography. Blowfish is a allow unfastened calculation and no longer but broke. Asymmetric cryptography is for the most part utilized for check and advanced marks. To legitimize that sender is the first verified gathering of information.

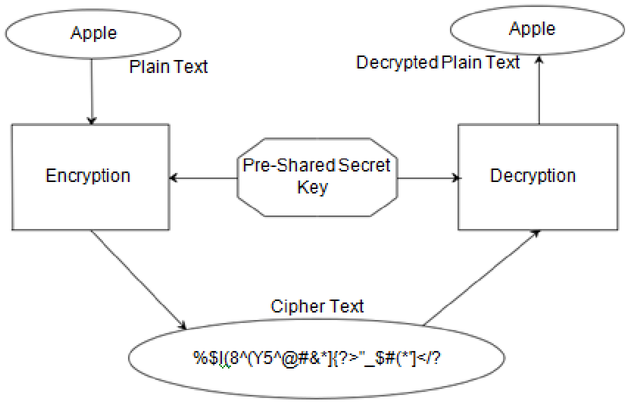

Figure 1. Basic Crypto System

A high speed and reliable crypto system using Blowfish algorithm is described in this paper. First chapter describes the fundamentals regarding cryptosystem and introduction to the Blowfish algorithm. Second chapter describes the literature review. Third chapter describes the basic structure and implementation of the Blowfish algorithm. Fourth chapter explains the actual proposed and construction of the high-speed crypto system using Blowfish algorithm and the next chapter describes the concluding remarks.

II.LITERATURE REVIEW

Russell K. Meyers et al proposed a Blowfish Cryptosystem, which works on information approximately assaults, at the aspect of information approximately a number of the human beings who've labored to investigate and strive to break blowfish. Mingyan Wang worked on unique password protection schemes. Here the writer delivered a password manage machine based totally on Blowfish Cryptographic Algorithm. The writer proposed and made some conclusions approximately the benefits of Blowfish Encryption Algorithm, defined some crucial facts of itsDesign and Performance Analysis of High-Speed Blowfish Cryptosystemencryption system, after which designed and accomplished the Passwords Management System (PMS).

Shun-Lung Su1et al worked on a novel 256-bits Block Cipher method, they proposed a 128-bit block cipher this is constructed with Feistel Network. The cipher, one of the very last applicants of AES, has a variable key duration of 128 ,192, and 256 bits. In this research, Twofish is accelerated to a 256-bit block encryption set of guidelines. Besides retaining the simple framework of Twofish, the style of rounds is reduced and enhance the framework of the feature to a higher protection stage.

Nadeem et al analyzed the famous secret key algorithms together with DES, 3DES, AES (superior encryption system), Blowfish. Their implementation and average performance turned into compared through encrypting numerous contents and sizes. The algorithms had been implemented on two one-of-a-type hardware structures to examine their ordinary overall performance. In the quit, the outcomes were supplied which concluded that the Blowfish turn out to be the quickest algorithm. Though safety changed into not catered for, in exercise, however, one would keep in mind the security first.

III. BLOWFISH ALGORITHM

Symmetric-key cryptography alludes to encryption strategies in which both the sender and collector share a similar key (or, less generally, in which their keys are unique, yet related in an effectively calculable manner). This was the main sort of encryption openly known. Symmetric key figures are actualized as either block ciphers or stream figures. A block cipher enciphers contribution to squares of plaintext instead of individual characters, the information structure utilized by a stream figure.

The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher plans which have been assigned cryptography measures by the US government (however DES's assignment was at long last pulled back after the AES was embraced). In spite of its belittling as an official standard, DES (particularly its still-affirmed and considerably more secure triple-DES variation) remains very prominent; it is utilized over a wide scope of utilizations, from ATM encryption to email protection and secure remote access. Numerous other block ciphers have been structured and discharged, with significant variety in quality. Many have been completely broken, for example, FEAL.

Stream cipher, as opposed to the 'square' type, make a discretionarily long stream of key material, which is joined with the plaintext a little bit at a time or character-by-character, to some degree like the one-time cushion. In a stream cipher, the yield stream is made dependent on a shrouded interior state which changes as the figure works. That inner state is at first set up utilizing the mystery key material. RC4 is a generally utilized stream cipher.

In cryptography, a block cipher is a deterministic calculation working on fixed-length gatherings of bits, called obstructs, with an unvarying change that is indicated by a symmetric key. Block ciphers are significant rudimentary parts in the structure of numerous cryptographic conventions and are broadly used to execute encryption of mass information.

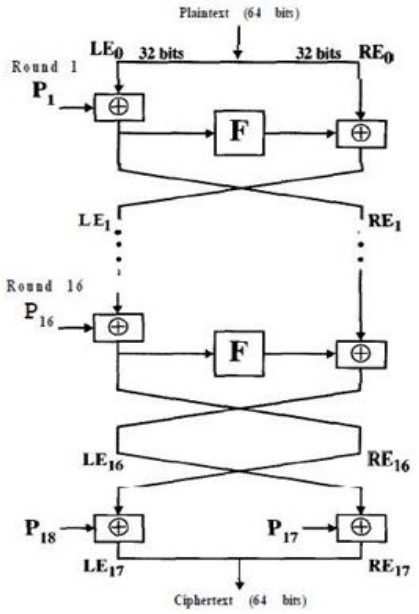

Figure 2. Blowfish Encryption

The present day plan of block ciphers relies upon at the idea of an iterated item discern. Product ciphers had been advocated and broke down through Claude Shannon in his essential production Communication Theory of Secrecy Systems to as it should be beautify safety via consolidating clear-cut obligations. Iterated product cipher does encryption in numerous rounds, every which makes use of an exchange subkey got from the number one key. An throughout the board utilization of such figures is known as a Feistel installation, named after Horst Feistel, and outstandingly finished inside the DES cipher.

The Blowfish set of rules should be productively implementable in custom VLSI gadget. There are numerous form hinders that have been exhibited to create strong figures. Huge numbers of these may be efficaciously actualized on 32-bit microchips. Enormous S-containers. Bigger S-bins are frequently impervious to differential cryptanalysis. A calculation with a 32-bit phrase period can make use of 32-bit S-packing containers.

Blowfish is a variable-duration key square determine. It would now not meet each one of the necessities for some other cryptographic ultra-modern pointed out above: it's miles low priced for applications wherein the key does now not exchange frequently, just like an interchange be part of or a programmed file encryptor. It is largely quicker than DES when performed on 32-bit microchips with large data systems.

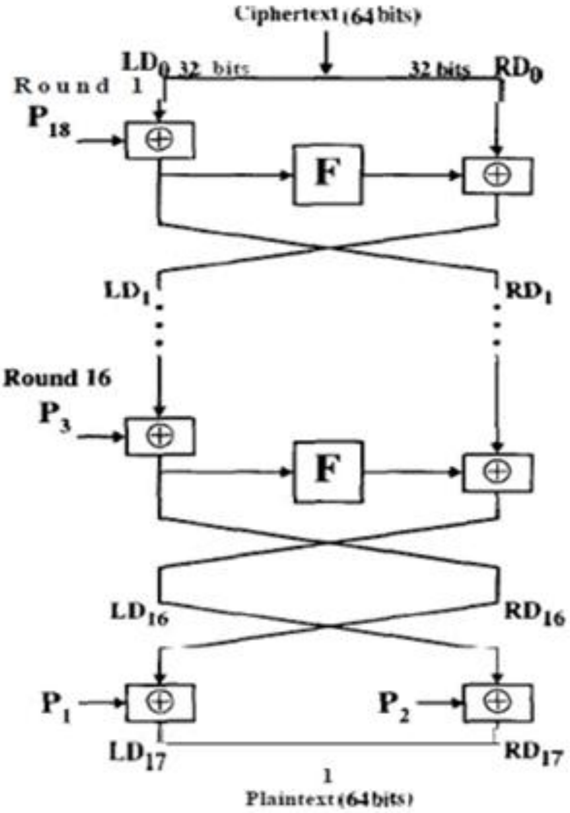

Figure 3. Blowfish Decryption

Blowfish is a variable-duration key, 64-bit block cipher. The set of rules includes elements: a key enlargement part and a records- encryption part. Key expansion converts a key of at most 448 bits into several sub key arrays totaling 4168 bytes. Data encryption takes region via a 16-spherical Feistel network. Each spherical includes a key-primarily based permutation, and a key- and informationestablished substitution. All operations are XORs and additions on 32-bit phrases. The only extra operations are 4 indexed array information lookups in step with round.

Blowfish makes use of a big variety of sub keys. These keys have to be pre-computed in advance than any data encryption or decryption. The P-array consists of 18 32-bit subkeys: P1, P2,..., P18. There are 4 32-bit S-containers with 256 entries each: S1,0, S1,1,..., S1,255; S2,zero, S2,1,..,, S2,255; S3,0, S3,1,..., S3,255; S4,zero, S4,1,..,, S4,255.

Blowfish is a Feistel network along side 16 rounds.

Algorithm way entails following steps:

The enter is a 64-bit records detail, x. Divide x into 32-bit halves: xL, xRxL = xL XOR Pi

xR = F(xL) XOR xR

Swap xL and xR

Swap xL and xR

xR = xR XOR P17

xL = xL XOR P18

Recombine xL and xR

Function F :

Divide xL into four 8-bit quarters: a, b, c, and d

F(xL) = ((S1,a + S2,b mod 232) XOR S3,c) + S4,d mod 232

IV.IMPLEMENTATION OF HIGH-SPEEDBLOWFISH ALGORITHM& RESULTS

The major principle in the back of Blowfish is that effortlessness of configuration yields a calculation this is every more clean and much less tough to execute. Using a streamlined Feistel shape, a essential S-field substitution and a essential P-container substitution. The structure may not incorporate any defects. A 64-bit rectangular duration yields a 32-bit word period and maintains up rectangular period similarity with modern calculations. Blowfish is something but hard to scale as much as a 128-bit rectangular, and down to littler square sizes..

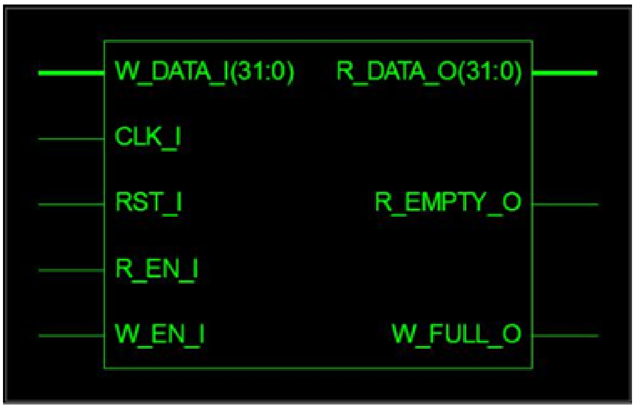

Figure 4. Schematic Diagram of FIFO

Figure four suggests the schematic diagram of FIFO which consists of 32 enter signals W_DATA_I(31:0) and 32 output pins R_DATA_O(31:zero) and clock sign and moreover manage alerts for reset (R_ST_I), have a look at allow (R_EN_I) for permitting the examine operation and write permit (W_EN_I) for allowing the write operation. It consists of more output manipulate signs which suggests the the popularity of FIFO R_EMPTY_O for receiver empty and W_FULL_O for write entire condition.

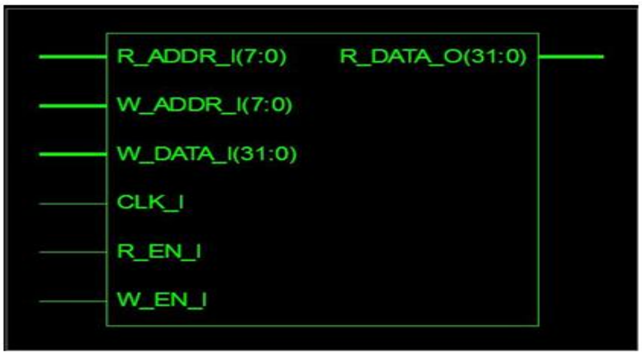

Figure 5. S-Box Schematic Representation

Figure 5 shows the schematic instance of S-Box. S-Box is the main logical block which implements unique competencies as defined in previous chapter. S-Box consists of 32 enter indicators W_DATA_I(31:zero) and 32 output pins R_DATA_O(31:zero) and one clock sign, have a look at enable (R_EN_I) for permitting the examine operation and write allow (W_EN_I) for allowing the write operation. It additionally includes allow sign. It includes 8 address strains for observe and writeR_ADDR_I(7:0) and W_ADDR_I(7:0) respectively. where it can address 28 address locations (256). S-Box is used to store sub keys of blowfish algorithm.

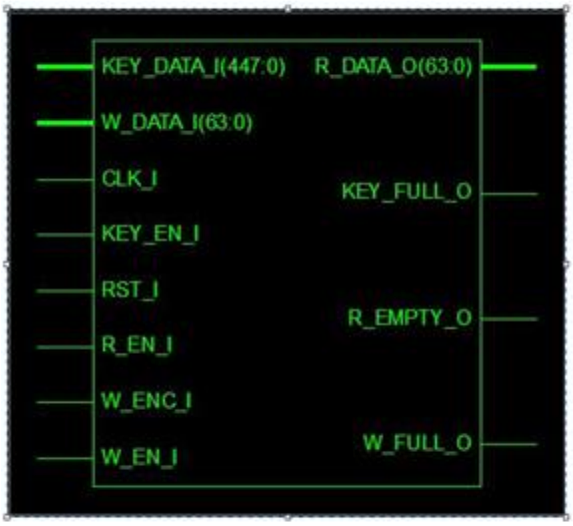

Figure 6. Blowfish cryptosystem

Table 1. Comparison table for different parameters.

Parameter	Blowfish	Proposed Algorithm
Critical path delay	3.5 ns	3.226 ns
Frequency (MHz)	296.12 MHz	298.15 MHz
Latency	35 cycles/sec	45 cycles/sec
Throughput	600 Mbps	2 Gbps
Throughput/slice	0.19 Mbps	2.5 Mbps

Table 1 indicates the comparative consequences of Blowfish encryption technique and the proposed immoderate-speed Blowfish encryption set of guidelines. Critical route postpone of the proposed approach is reduced with the useful resource of 8 percent and on the almost equal frequency is decided 45 cycles in keeping with 2nd in proposed approach. Throughput of the proposed approach is in many instances immoderate as compared with traditional set of rules. Per every slice also there's a big boom in throughput is located. All the comparative outcomes are tabulated in Table 1.

Figure 6 shows the black field representation of Blowfish crypto device. The schematic of Blowfish cryptosystem includes 64 enter signs W_DATA_I(sixty three:zero) and sixty 4 output pins R_DATA_O(sixty 3:0) and one clock signal, examine enable (R_EN_I) for permitting the examine operation and write allow (W_EN_I) for permitting the write operation. It moreover carries permit signal. It also carries 448 duration of key data KEY_DATA_I(447:zero) and manage signals for key entire KEY_FULL_O and receiver empty R_EMPTY_O and Write entire W_FULL_O.

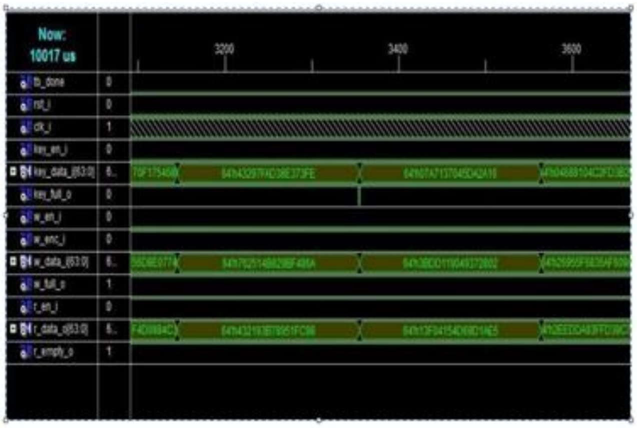

Figure 7. Simulation results showing Blowfish cryptosystem

Figure 7 shows the simulation results of the Blowfish set of rules. Entire shape is described the usage of Verilog HDL and is implemented on Spartan 3E FPGA. Simulation outcomes suggests the plain text and the cipher textual content. Decryption set of regulations is applied as separate block and the identical cipher text is given as enter thru FIFOs. Two FIFO are used to preserve undeniable textual content and cipher text and a few different FIFO is used to keep the decrypted textual content. Keys are generated with the help of Pi. Because Pi has a by no means ending and non-repeating fractional element, Pi fractional component in binary is used to generate S-Box keys.

V. CONCLUSION

Blowfish Encryption scheme and Decryption is applied the use of VHDL language. This is a excessive secured algorithm. Software cryptanalysis of the form of complex set of policies can be very complicated issue and is taking large quantity of time to finish all of the vital procedure steps inside the algorithm. It can be very lots vital to enforce the kind of complex structure on hardware. Hardware implementation of this sort of immoderate secured set of rules is quite critical for immoderate tempo programs. Because of the hardware implementation of the set of rules, there's no need of any external platform to run the set of rules, and the obvious textual content is encrypted internal fraction of seconds. Simulation consequences shows that this algorithm it is able to encrypt a plain text in less than 7000 ns of time. There is an big boom in throughput is discovered inside the proposed structure.

VI. ACKNOWLEDGMENT

This research work is partially supported by CMR College of Engineering & Technology. We thank our management and colleagues from CMR College of Engineering & Technology, who provided their greatest support while doing this research work.

VII. REFERENCES

[1] A. Nadeem and M. Y. Javed, “A performance comparison of data encryption algorithms,” in 2005 international conference on information and communication technologies, 2005, pp. 84–89.

[2] L. Domnitser, A. Jaleel, J. Loew, N. Abu-Ghazaleh, and D. Ponomarev, “Non-monopolizable caches: Low-complexity mitigation of cache side channel attacks,” ACM Transactions on Architecture and Code Optimization (TACO), vol. 8, no. 4, p. 35, 2012.

[3] Y. Wang, “Password protected smart card and memory stick authentication against off-line dictionary attacks,” in IFIP international information security conference, 2012, pp. 489–500.

[4] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, “The 128-bit blockcipher CLEFIA,” in International workshop on fast software encryption, 2007, pp. 181–195.

[5] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, “A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish,” Procedia Computer Science, vol. 78, pp. 617–624, 2016.

[6] O. Kara and C. Manap, “A new class of weak keys for blowfish,” in International Workshop on Fast Software Encryption, 2007, pp. 167–180.

[7] P. C. Mandal, “Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish,” Journal of Global Research in Computer Science, vol. 3, no. 8, pp. 67–70, 2012.

[8] T. Nie, C. Song, and X. Zhi, “Performance evaluation of DES and Blowfish algorithms,” in 2010 International Conference on Biomedical Engineering and Computer Science, 2010, pp. 1–4.

[9] J. Thakur and N. Kumar, “DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis,” International journal of emerging technology and advanced engineering, vol. 1, no. 2, pp. 6–12, 2011.

[10] M. A. Kumar and S. Karthikeyan, “Investigating the efficiency of Blowfish and Rejindael (AES) algorithms,” International Journal of Computer Network and Information Security, vol. 4, no. 2, p. 22, 2012.

[11] B. Schneier, “Description of a new variable-length key, 64-bit block cipher (Blowfish),” in International Workshop on Fast Software Encryption, 1993, pp. 191–204.

[12] X. He, A. Machanavajjhala, and B. Ding, “Blowfish privacy: Tuning privacy-utility trade-offs using policies,” in Proceedings of the 2014 ACM SIGMOD international conference on Management of data, 2014, pp. 1447–1458.

[13] T. Nie and T. Zhang, “A study of DES and Blowfish encryption algorithm,” in Tencon 2009-2009 IEEE Region 10 Conference, 2009, pp. 1–4.

[14] P. C. Mandal, “Superiority of Blowfish algorithm,” International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, no. 9, 2012.