INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 01, January 2024, pp : 515-519

e-ISSN : 2583-1062

Impact Factor : 5.725

DESIGN AND IMPLEMENTATION OF 16-BIT HIGH SPEED CARRY SELECT PARALLEL PREFIX ADDER

Gangolu Rajesh[1], Raju Thommandru[2], Shaik Mahaboob Subhani[3]

[1,3]Assistant Professor, Department of ECE, Chalapathi Institute of Technology, Mothadaka, Guntur, Andhra Pradesh, India.

[2]Associate Professor, Department of ECE, Chalapathi Institute of Technology, Mothadaka, Guntur, Andhra Pradesh, India.

ABSTRACT

Many applications, including health-monitoring and biometric data based recognition system, need short-term data security. To design short-term security based applications, there is an essential need of high-performance, low cost and area-efficient VLSI implementation of lightweight ciphers. Data Encryption Standard (DES) is well-suited for the implementation of low-cost lightweight cryptography applications. In this paper, we propose an efficient VLSI architecture for DES algorithm based encryption/decryption engine. Depending upon the encryption/decryption needs, the same set of architecture performs both encryption and decryption operations. Design of area efficient and less delay utilization is a major concern for the VLSI (Very Large Scale Integration) circuit designer. This paper presents an efficient high-speed VLSI-Architecture for Data Encryption Standard by using a Carry Select Parallel Prefix Adder (CSPPA). This results show that the suggested design has low delay and area when compared with other available designs.

Keywords: Data Encryption Standard (DES), VLSI (Very Large Scale Integration), Carry Select Parallel Prefix Adder (CSPPA), cryptography, encryption/decryption.

1. INTRODUCTION

In present day scenario, VLSI circuits with low power, and low area are need of the hour. At the same time delay remains an important parameter to enhance speed of circuit. For any VLSI data path design, adders and multipliers form an integral part of circuit and capable of deciding performance and efficiency of circuit [1]. This paper aims at implementation of power and area efficient adder circuits. In 1962, Carry select Adder (CSLA) was designed.

From the literature it is known that Conventional CSLA is amongst the fastest adders since it overcomes the issue of carry propagation. For two probable values of carry (i.e. ‘1’ and ‘0’) parallel summation is calculated and multiplexer selects the correct sum based on previous carry generated [2]. A number of adder architectures already exist in literature and this paper aims at optimizing the concept of all architectures in one to gain the maximum optimization.

Secure communication is crucial in modern authentication-based applications like bank transactions, electronic mail, and audio/video conferencing. Cryptography is essential for ensuring no unauthorized person can access the communicated information over an unsecure medium. The implementation of cryptography algorithms on the hardware is essential for achieving optimal performance of system by maintaining the system physical security [3]. Cryptography is a science that enables the confidentiality of communication through an insecure channel. The basic cryptographic processes consist of conversion of plaintext into a ciphertext by the process of encryption and retrieval of the plaintext from the ciphertext by decryption process. The cryptographic process is used for authentication in many applications such as: in bank cards, wireless telephones, e-commerce, pay-TV etc. Encryption/decryption is also required for the access control in many systems, such as carlock systems, lifts, metro trains, etc. Nowadays it is widely used for electronic payment in prepaid telephone cards, e-cash cards etc. Cryptanalysis manages the investigation and examination of cryptographic calculations in a down to earth approach to comprehend their working and discover the vulnerabilities to break them. Cryptanalysis is used by military and some reconnaissance activities subsidized by huge associations so as to test security basic frameworks. In addition, programmers additionally use cryptanalysis to misuse vulnerabilities in various frameworks and sites [4]. The way toward performing cryptanalysis isn't that basic, but it requires mastery in the field of science and inside and out understanding. In the old occasions, cryptanalysis was just intended to provide the key. This key will decode a message by contemporary cryptography. In this cryptography arithmetic and rapid PCs will break an encryption calculation [5]. It is also used in applications including health-monitoring and biometric data based recognition applications need short-term security. In addition, with advent of embedded computing and omnipresent smart embedded devices, there is a need of highperformance, area-efficient and low cost very-large-scale integration (VLSI) implementation of lightweight ciphers such as data encryption standard (DES). For the implementation of low-cost lightweight cryptography, the DES algorithm is very well suited. DES algorithm is a symmetric block cipher and it provides adequate level of security with low hardware cost. Though, the 56-bit key limits the security level, yet, brute-forcing this key space using software requires a few months alongwith several computing engines [6]. Although, DES has evolved into the advanced encryption standard (AES), nonetheless, many applications continue to rely on DES for cryptography and information security. Therefore, the designers and implementers continue to support for efficient architecture for the DES in many short-term security applications. Thus, there is always a need of optimized, high-performance hardware implementation of DES and other lightweight ciphers.

Adders have become a critical component in the effective implementation of arithmetic units. Adders are utilized not just in the arithmetic logic unit, but also in other parts of the processor in many applications [7].High-speed adders are highly desirable in the present day scenario, though power (or energy) and silicon area are equally vital. Spectrum sensors used in intelligent cognitive-radio environment as well as Internet of Everything (IoE) devices focused on physical interfaces are largely-explored research areas in the recent time. Hardware for the algorithms of such applications is basically focused on sensing and actuating where the response time is key component to be optimized for real-time interfaces. Thereby, the design of highly optimized adders in terms of speed play significant role in the present era and hence this paper focuses in the design of same. With tolerable degradation in accuracy and performance, it is feasible to conceive high-speed, low power and area efficient design using parallel prefix adder.

In various VLSI designs adders are most frequently used. The binary adder is the most important element in most digital circuit designs including digital signal processors (DSP), microprocessor data path units. In many applications of digital systems several types of adders can be used such as half & full adders, ripple carry adders, carry look ahead adders etc. Among all these adders Carry Look Ahead adder has an improved delay compared to half adder, full adder and ripple carry adder. The Carry Look Ahead (CLA) adder improves the speed by reducing the amount of time required to determine the carry bits. To propagate the carry to the next stages it introduced two new signals called Propagate and Generate (G, P).But the problem with the CLA is, as the number of input bits is going to be increased the delay of adder becomes worst. To eliminate this problem engineers devised new adders called Parallel prefix adders. The logarithmic delay of the parallel prefix adders improves the speed efficiently as well as requires less area requirements.

2. LITERATURE SURVEY

CRS Bhardwaj et. al. [8], Elaborate the Modification Of DES Algorithm analyzes the change of DES computation, which is the examination of data encryption, an advancement that obliges a protected, secure, and private information trade. W. Stallings et. al. [9] Encryption algorithm performs various mathematical and logical functions on the plaintext by using the key. Cipher data is the encrypted message produced by encryption algorithm by using the key and the plain text. Decryption algorithm is employed on cipher data and performs reverse action to generate the plain text. The symmetric key encryption algorithm shares the same key between sender and receiver and a strong algorithm for encryption and decryption processes is essential to provide an efficient security mechanism. N. A. Saqib, F. Rodrıguez-Henriquez, and A. Dıaz-Perez et. al. [10] presents that the encryption hardware proposed does not become a bottleneck even for the networks capable of transferring several gigabits per second. A compact and efficient reconfigurable hardware implementation of DES algorithm is presented on a VirtexE XCV400e device. S. Landau et al.,[11]proposed a simple and efficient VLSI architecture for computation of DES algorithm. The proposed architecture requires nineteen clock cycles to encrypt a plaintext into ciphertext. The decryption process is identical to encryption operation and it completes the decryption process in nineteen clock cycles. The key generation process is realized in a combinational datapath and it provides all the required sixteen round keys to the encryption/decryption block in the first cycle of the clock. By this, it makes the decryption block to start the decryption process by using the last round key, which is mandatory as per the DES decryption algorithm. To implement an S-Box, five multiplexers (MUXs) are used. Out of the five MUXs, four MUXs are of 4-bit, 16-to-1 MUXs and one 4-bit, 4-to-1 MUX. To make the design work in pipelined mode the inputs and outputs are registered. Ali Makhmali, Hajar Mat Jani et. al. [12] illuminates the execution and respond in due order regarding handle these two issues. These issues at first drove us to play out a close audit on a couple of encryption computations, and in this way, to find the most fitting one; and second, to find the best organization structure of data to ensure a sensible level of security for the clients of the online application. R. UMA,Vidya Vijayan, M. Mohanapriya, Sharon Paul et. al., [13] presents Area, Delay and Power Comparison of Adder Topologies. This paper presents the pertinent choice for selecting the adder topology with the tradeoff between delay, power consumption and area. The adder topology used in this work are ripple carry adder, carry look ahead adder, carry skip adder, carry select adder, carry increment adder, carry save adder and carry bypass adder. The module functionality and performance issues like area, power dissipation and propagation delay are analyzed at 0.12µm 6metal layer CMOS technology using microwind tool.

3. METHODOLOGY

In Fig.1 flowchart of design and implementation of 16-Bit high speed carry select parallel prefix adder is observed.

Here in this VLSI architecture for data encryption and decryption operations use the same set of hardware building blocks. This system initially takes 2 inputs, pre-processing stage, carry generation stage, black and gray cells, post-processing stage and result.

Pre-processing requirements are those tasks that are mostly input independent and therefore they are required to compute only once in the beginning. The hardware design is the part that uses the pre-processing results and performs the recognition in 2n time units.

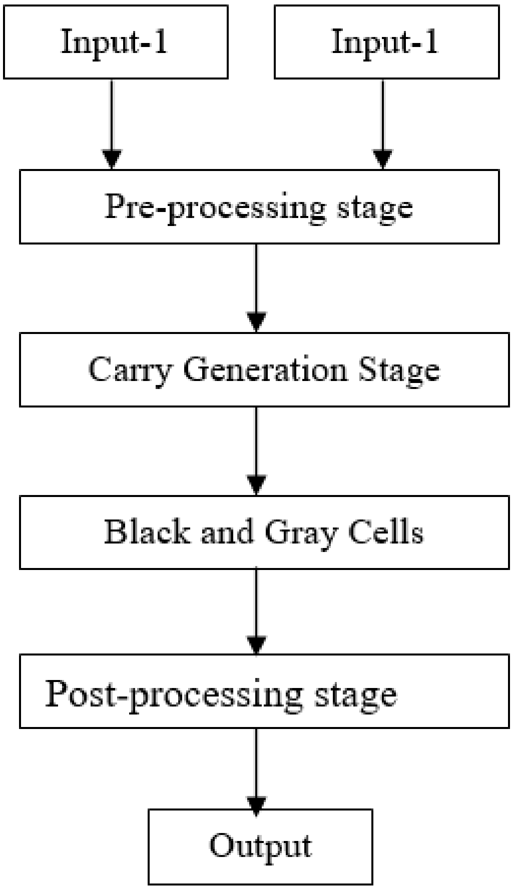

Fig.1: Flowchart of Design And Implementation of 16-Bit High Speed Carry Select Parallel Prefix Adder

Carry Generation Stage: This stage computes the carries corresponding to each bit. Execution of these operations is carried out in parallel. After the computation of carries in parallel they are segmented into smaller pieces. We uses carry propagate and generate signals as intermediate signals which are given by the logic equations

CPi:j = Pi: k +1 and Pk: j ….(1)

CG i:j=Gi:k+1 or

(Pi:k+1and Gk:j) ….(2)

Black Cell- The black cell takes the two pairs of input signals (gi, pi) and (gj, pj) and computes generate and propagate bits using the following equations.

g= gi+ pi .gj P=pi .pj ---(3)

Gray Cell- This block takes two pairs of input signals (gi, pi) and (gj , pj) and generates the single output signal g.

g=gi+ pi .gj --- (4)

Post Processing Stage: This is the final stage of all adders of this family which computes the sum bits.

Ci-1= (Pi and Cin) or Gi …. (5)

Si =Pi Xor Ci-1 …. (6)

After the post processing stage final output is evaluated.

4. RESULT ANALYSIS

In this section performance analysis of design and implementation of 16-Bit high speed carry select parallel prefix adder is observed.

Table.1: Performance Analysis

Parameters	Existing System	Proposed System
Delay (ns)	95476	79855
Area (KB)	84512	66579

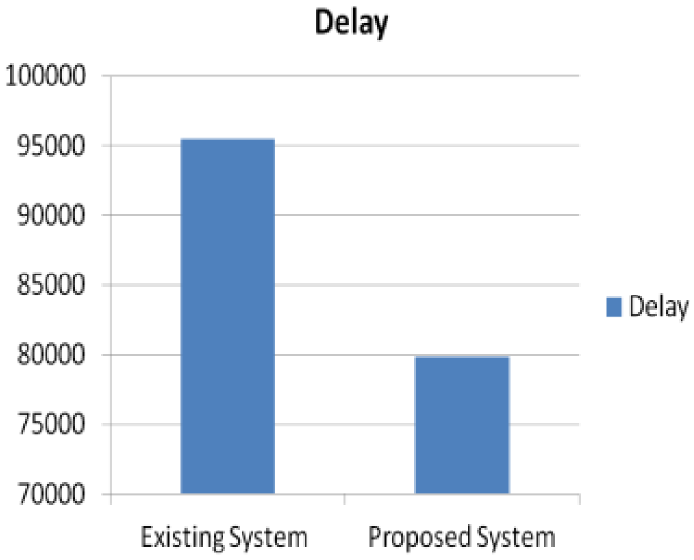

Fig.2: Delay comparison graph

In Fig.2 delay comparison graph is observed between existing system and proposed system. The proposed system shows low delay

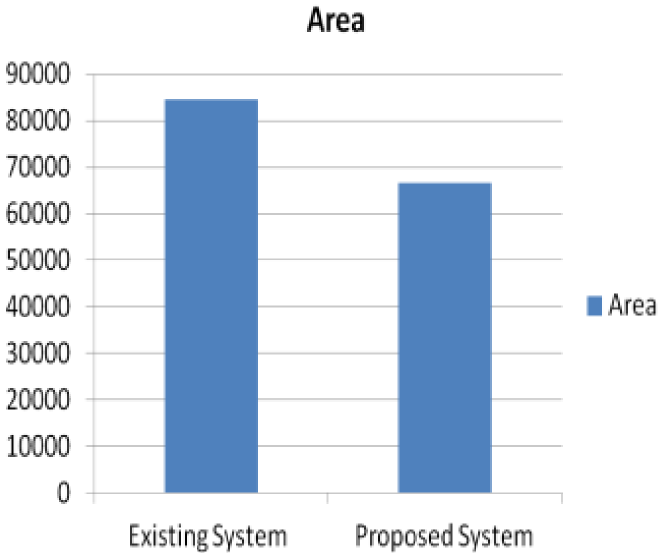

Fig.3: Area comparison graph

In Fig.3 area comparison graph is observed between existing system and proposed system. The proposed system shows low area.

5. CONCLUSION

In this analysis, they have designed an efficient VLSI architecture by using a carry select parallel prefix adder. This architecture is very regular and it requires very low amount of hardware resources, therefore it can be efficiently utilized in lightweight cryptography applications. The design has been modeled in the VHDL language and it has been synthesized for Xilinx Virtex-5. The performance of DES using CSPPA is evaluated in terms of delay and area.

6. REFERENCES

[1] Asha Cn, Jayalaxmi H, Sapna Kumari C, Nagapushpha Kp, “Three Operand Binary Adder Of Low Power And High Speed Vlsi Architecture”, Journal of Tianjin University Science and Technology ISSN (Online): 0493-2137 E-Publication: Online Open Access Vol:55 Issue:04:2022 DOI 10.17605/OSF.IO/CFA43

[2] Sarita Shambharkar, Archana khandait, “Design of efficient adder for high speed”, International Journal of Creative Research Thoughts (IJCRT), IJCRT2107508, 2021 IJCRT, Volume 9, Issue 7 July 2021

[3] Satyandra Bhati, Neeraj Sharma, Meetu Nag, “Performance Analysis of High Speed and Low Power Binary Adders”, IOP Conf. Series: Materials Science and Engineering, 2021, doi:10.1088/1757-899X/1224/1/012026

[4] A. Radha, K.S.N. Murthy, “Design of a High Speed and Area Efficient Novel Adder for AES Applications”, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-2, July 2019

[5] Nithya. J, Ramesh S.R, “Design of Delay Efficient Hybrid Adder for High Speed Applications”, 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), 978-1-5386-9533-3/19

[6] K. Ram Gavali and P. Kadam (2016), ‘VLSI Design of High Speed Vedic Multiplier for FPGA implementation’, 2nd IEEE International Conference on Engineering and Technology.

[7] M. Akila, C. Gowribala and S. Maflin Shaby (2016) , ‘Implementation of High Speed Vedic Multiplier using Modified Adder’, International Conference on Communication and Signal Processing, pp. 2244-2248.

[8] CRS BHARDWAJ, Modification Of Des Algorithm, International Journal Of Innovative Research & Development, Nov 2012, Vol 1,Issue 9,Page 495.

[9] W. Stallings, L. Brown “Computer Security Principle and Practice,” pp.593-600, ISBN: 978-0-13-600424-0, Pearson Education, 2008.

[10] N. A. Saqib, F. Rodrıguez-Henriquez, and A. Dıaz-Perez, “A compact and efficient fpga implementation of the DES algorithm,” 2004.

[11] S. Landau, “Standing the test of time: The data encryption standard,” Notices of the AMS, vol. 47, no. 3, Mar. 2000, pp. 341-349.

[12] Ali Makhmali, Hajar Mat Jani, Comparative Study On Encryption Algorithms And Proposing A Data Management Structure, International Journal Of Scientific & Technology Research, Volume 2, Issue 6, June 2013.

[13] R. UMA,Vidya Vijayan, M. Mohanapriya, Sharon Paul, “Area, Delay and Power Comparison of Adder Topologies”, International Journal of VLSI design & Communication Systems (VLSICS) Vol.3, No.1, February 2012, DOI:10.5121/vlsic.2012.3113