International Journal of Scientific Engineering and Research (IJSER)
ISSN (Online): 2347-3878
Impact Factor (2018): 5.426

Review Paper on Cryptography and Data Encryption Standard Method based FPGA

Vinay Kumar Maurya[1], Prof. Rajesh Sharma[2]

[1]M.Tech Scholar, VLSI, Truba College of Science & Technology, Bhopal, Madhya Pradesh, India
[2]Assistant Professor, ECE, Truba College of Science & Technology, Bhopal, Madhya Pradesh, India

Abstract: ***Secure correspondence is the prime prerequisite of each communication. In today's reality the security has turned into the real part of life. It can be accomplished by different systems such as cryptography and biometrics. A Field-Programmable Gate Array (FPGA) is a semiconductor device containing programmable rationale segments called rationale squares, and programmable interconnects. Rationale squares can be customized to perform the capacity of fundamental rationale gates, for example, AND, and XOR, or more unpredictable combinational capacities, In this review paper, we are going to present the brief introduction of cryptography and DES method based FPGA along with the work done in this field.***

Keywords: Cryptography, DES, secure communication

1.Introduction

This paper includes the introduction of various cryptography algorithms and approaches used for data security. Their design styles and applications have also been included in this paper. These days cryptography has a primary part in installed frameworks outline. As the quantity of devices and applications which send and get information are expanding quickly, the information exchange rates are getting to be higher. In numerous applications, this information requires a secured association which is generally accomplished by cryptography. Numerous cryptographic calculations were proposed, for example, the Data Encryption Standard (DES), the Elliptic Curve Cryptography (ECC), the Advanced Encryption Standard (AES) and different calculations. Numerous analysts and programmers are continually attempting to break these calculations utilizing savage compel and side channel assaults. A few assaults were effective as it was the situation for the Data Encryption Standard (DES) in 1993, where the distributed cryptanalysis assault [22] could break the DES. The Enhanced Data Encryption Standard (DES) is viewed as these days as one of the most grounded distributed cryptographic calculations, where it was embraced by the National Institute for Standards and Technology (NIST) after the falling flat of the Data Encryption Standard (DES). In addition, it is utilized as a part of numerous applications, for example, in RFID cards, ATM Machines, mobile phones and expansive servers. Because of the significance of the DES calculation and the various applications that it has, the principle worry of this proposition will be displaying new proficient equipment usage for this calculation. Equipment executions for the DES calculation fluctuate as indicated by the application. While a few applications require high throughputs as in e-trade servers, others require medium throughput range as in outlines for phones [17]. A few others require low region usage to be utilized as a part of low power application as in RFID cards. Numerous equipment outlines where proposed for the DES calculation. Some of these outlines focused on rapid applications as on top of it unrolled 128 bits plans [2], [3] and [5], while others focused on medium and low territory executions as in the plans [14], [15] and [17]. As every application requires the DES to have diverse pace and range, this postulation presents two new equipment usages for the DES calculation. The primary equipment usage is a rapid 128 bits DES encryption with new blending and pipelining systems, while the second equipment execution is a medium throughput 32 bits DES outline with effective assets sharing and inward pipelining strategies. Both outlines have accomplished better efficiencies and exhibitions contrasting with past DES equipment plans.

1.1 Cryptography

It is a method used to stay away from an unapproved access of information. It serves to give responsibility reasonableness and precision furthermore give privacy. Extensively, four various types of individuals contributed their endeavors in this method and are: (i) Military, (ii) The Diplomatic Corps, (iii) Diarists, and (iv) Communications System. Cryptography includes two essential operations also, is named as encryption and key administration. Data/information can be scrambled utilizing a cryptographic calculation by different keys. The security of cryptographic framework is not just reliant on the encryption calculation; it likewise relies on the keys utilized for the encryption. Cryptography is an important technique to protect digital information data. In recent years due to the heavy increase in the volume of information data, secure and rapid cryptographic algorithms were developed to combat security threats and security measures were considered to be necessary wherever, digital data's transactions have to be processed. The high diversity found in security applications presents an additional challenge, not only because highly secure algorithms are required, but for some applications and for others high performance, less space. In that scenario, cryptographic designers have explored not only realizations on software platforms, but also on classic hardware or reconfigurable hardware platforms as well. Implementing cryptographic algorithms on reconstructed hardware has major advantages over VLSI (large-scale integrated circuits) and software platforms because they offer the same high speed and high flexibility as VLSI. VLSI implementations are fast, but must be designed in all ways, from behavioral description to physical layout. They have to follow an expensive and time consuming construction process. Software implementations provide high flexibility, but they are not fast enough for time-critical

applications. Reusable devices, on the other hand, are attractive because VLSI reduces design and manufacturing time and cost. In addition, they provide high potential for reproduction and experimentation on multiple structures or for multiple modifications of a single structure. Among the various cryptographic algorithms, the most popular example in the field of symmetric ciphers is the Data Encryption Standard (DES) algorithm [1, 2], developed by IBM in the mid-seventies. The DES algorithm consists of logical operations, permutations, alternatives, shift operations, and many bit-level operations. Platform: Reusable hardware using software [1–5], VLSI [4–and] and FPGA devices [9–13, [, 14]. In this paper we present an efficient and compact DES architecture designed specifically for reusable hardware platforms. The DES implementation presented in this paper differs from other previous works in the following areas: it uses an eight DES S-box parallel structure, resulting in no significant encryption / decryption paths.

These key ranges are constantly protected from programmers and are called mystery keys. Keys play an important role in the encryption process, which is a fundamental part of cryptography [31]. Because of channel debilitations now and then the transmitted information and/or key may get tainted. On the off chance that it is somewhat changed or debased, the information won't be recouped; along these lines, key should be transported over the secured channel. The recurrence of utilization of a cryptographic key dependably has an immediate relationship to how regularly the key ought to be changed. Encryption calculations can be hacked by using supercomputer which gives quick speed and permits the programmer to utilize more changes and blends in a predetermined time. Cutting edge time relies on remote correspondence and very nearly all the electronic stores are being done on the web. With a specific end goal to secure the same and keep up the clients' security; cryptography is the best arrangement because of their better reaction even in the vicinity of admonitory. For better security, either more number of keys is utilized or the length of the existing keys is expanded. In both the methodologies the overheads are expanded, consequently, the best thought is to utilize sub-keys. Sub-keys are utilized just for such hubs which are assaulted by the programmer.

The sub keys are constantly gotten from the fundamental key which helps in diminishing the overheads. The fundamental cryptographic model has been appeared in figure 1.1. It includes encryption and unscrambling area; at first, the information has been scrambled by the assistance of key and further transmitted over the web. At last, it has been gotten and the scrambled information is decoded with the assistance of same or distinctive key. The key is any worth and/or word and is utilized as a part of both the areas for encryption also, unscrambling reason.

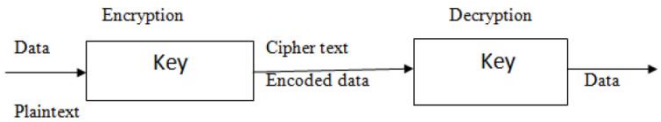

Figure 1: Block diagram of Cryptographic Model

Following are two types of key-based encryption algorithms which are: symmetric and asymmetric algorithms. Symmetric algorithms use the same key for encryption and decryption, whereas asymmetric algorithms use different keys for encryption and decryption.

1.2 Need of Cryptography

As every one of the associations, for example, banks, railroad, military, telecom, and so on depends upon remote methodologies and are interested in all the PC and the systems (LAN, MAN and WAN). Their exchange of trusts, data and information all are done on the web. Secured financing also, E-sends are the real prerequisite of all the above said associations; in this way, it is exceptionally crucial to shield the information from the interlopers. Electronic information move is utilized as a part of all the present applications and it incorporates the security of ATM cards, PC passwords, and electronic trade. Passwords are bad so far for the assignment [32] because of their short range; in this manner, cryptography has wide future on the grounds that this procedure can have the capacity to with stand against the different assaults.

1.3 Key Terms Used in Cryptography

Encryption Algorithm is a system to change over the plain content into the figure content with the assistance of symmetric and/or deviated keys. Ciphertext is a structure which can't be effortlessly comprehended by unapproved individuals.

Cryptosystem is equipment or programming execution of cryptography is that changes a message to ciphertext and back to plaintext. A cryptosystem comprises of three calculations: one for key era, one for encryption, [33] and one for unscrambling. The term figure (now and again figure) is regularly used to allude to a couple of calculations, one for encryption and one for unscrambling. Cryptosystem is frequently utilized when the key era calculation is essential.

Cryptanalysis is a practice of obtaining plaintext from ciphertext without a key or breaking the encryption. Cryptanalysis refers to the study of ciphertext, ciphers or cryptosystems with an aim to find infirmity that will permit retrieval of the plaintext from the ciphertext, without necessarily knowing the key or the algorithm. This is known as breaking [31] the cipher, ciphertext, or cryptosystem.

Ciphertext is the information in encoded or unintelligible configuration. Plaintext is the thing that you have before encryption, and ciphertext is the encoded result. The term figure is some of the time utilized as an equivalent word for ciphertext, however it all the more legitimately means the strategy for encryption as opposed to the outcome. Cryptology is the investigation of both cryptography and cryptanalysis.

Encipher is the demonstration of changing information into a mixed up organization. Encipher is the demonstration of changing information into a decipherable organization in a manner that the examination of archives written in antiquated dialects, where the dialect is obscure, or information of the dialect has been lost. Key Secret is an

arrangement of bits and guidelines that represents the demonstration of encryption and unscrambling. The keys should be ensured as they are being transmitted keeping in mind they are being put away on every workstation and server. The keys [33] should be created, wrecked, and recuperated legitimately. Key administration can be taken care of through manual or programmed forms.

The classification of data that cryptography can give is helpful not just to the genuine purposes of averting data wrongdoings e.g. the robbery of competitive advantages or unapproved exposure of delicate restorative records additionally for illegitimate purposes e.g., protecting from law implementation authorities a discussion between two terrorists wanting to bomb a building. With a specific end goal to accomplish the same one can utilize two procedures, (i) one can utilize imperceptible ink for composing the message or can send the message through the private individual, and (ii) utilization of logical methodology called "Cryptography". The crucial and established undertaking of cryptography is to give privacy by encryption routines. It is utilized as a part of uses present in innovatively propelled social orders; it incorporates the security of ATM cards, PC passwords, furthermore, electronic trade. In any case, the most perceived type of cryptography is its utilization enciphers and unravels data, along these lines keeping its substance made preparations for unapproved divulgence. There are two classes of key- based encryption calculations: symmetric and awry calculations. Symmetric calculations utilize the same key for encryption and decoding, while deviated calculations use diverse keys for encryption and decoding. Preferably it is infeasible to register the unscrambling key from the encryption key.

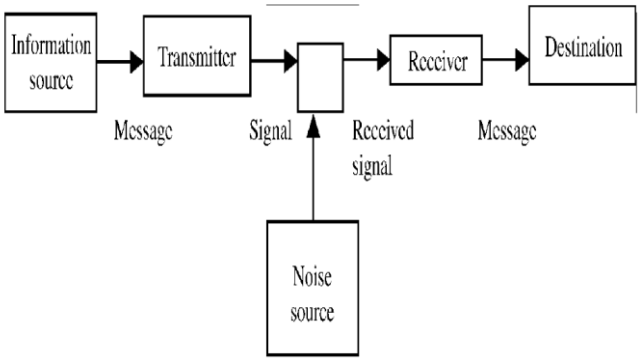

Figure 2: Block diagram of secured communication

1.4 Data Encryption Standard

During early 1970's, IBM developed Data Encryption Standard as a symmetric-key cryptography algorithm. This algorithm was adopted by the National Institute of Standard and Technology (NIST) in 1977, where it was published in the Federal Information Processing Standard (FIPS) Publication 46 [20]. The DES consists of 64 bits data block with key size of 56 bits, where 16 encryption rounds will be applied to the data to complete the encryption process.

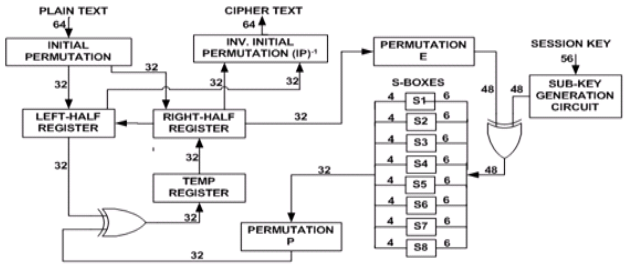

Figure 3: DES Algorithm

The DES algorithm starts to fail after several published brute force attacks. The linear cryptanalysis attack [22] could break the DES and made it insecure algorithm. The NIST started to search for another algorithm to replace the DES, where the Rijndael cipher was selected as the new Advanced Encryption Standard (AES).

1.5 Types of Ciphers

Substitution Cipher It is the one in which the letter of plaintext are supplanted by other letter or by numbers or images such process are known as substitution procedures [35]. There is different substitution procedures are as per the following:

Caser Cipher: It has been found by Julius Caser. The Caesar figure includes supplanting every letter of the letters in order with the letter standing three places further down the letters in order.

Mono alphabetic Cipher:

In mono alphabetic figure the figure content can be any stage of the 26 alphabetic.

Transposition Cipher In the transposition strategies are altogether different sort of performing so as to map is accomplished some kind of stage on the plaintext letters. This strategy is alluded as transposition figures. The easiest such figure is the rail wall strategies in which plaintext is composed in corner to corner and afterward read off as a succession of columns [31, 35]. In a transposition figure, stage is utilized, implying that letters are mixed. The key decides the positions that the characters are moved to, as showed.

2. Literature Review

Information Encryption Standard (DES) is the most surely understood cryptographic system in history [1]. It starts with the work of Feist el at IBM in the mid 1970s and coming full circle in 1977 with the appropriation as a U.S. Government Information Processing Standard for encoding unclassified data. The most striking advancement in the historical backdrop of cryptography came in 1976 when Diffie and Hellman distributed an exchange [2]. Prior to the cutting edge period, cryptography was concerned exclusively with message classification i.e. encryption transformation of messages from the fathomable structure into a tremendous one and back again at the flip side, rendering it mixed up without mystery information. In late

decades, the field has extended past classification worries to incorporate methods for verification, advanced marks, intuitive proofs, and secure calculation.

Ruth M. Davis [3] gives an equipment implementable calculation to enciphering information, which has been embraced as a Federal standard to give an abnormal state of cryptographic insurance against different assaults.

Whitfleld Diffie et. al [4] portrays cryptographic innovation, which inspects the powers driving open advancement of cryptography. The paper depicts how one can secure the message over the phone lines.

Ingrid Verbauwhede [5] portrayed Security and Performance Optimization of a New DES Information Encryption Chip. Novel CAD instruments are utilized at diverse strides as a part of the outline process for reproduction. The outcome is a solitary chip of 25 mm in 3-pm twofold metal CMOS. Usefulness tests demonstrate that a clock of 16.7 MHz can be connected, which implies that a 32-Mbit/s information rate can be accomplished for every one of the eight byte modes.

James E. Katz [6] gives Social Aspects of Telecommunications Security Policy that depicts a framework that offers a mixed bag of helpful and effective administrations while meeting the honest to goodness necessities of the person for protection and of society for security.

H. Bonnenbergt [7] portrayed the VLSI execution of another square figure. The chip that runs with a most extreme clock recurrence of 33 MHz allowing an information change rate of more than 55 Mbits/s performs information encryption and unscrambling in a solitary equipment unit.

K.H. Mundt [8] introduced superscript ASIC innovation that encouraged another device family for information encryption in which semi-custom cell-based ASIC innovation is portrayed to get 100Mbits/s encryption speed on silicon applying 1 micron configuration rules.

C. Boyd [9] gives the advanced information encryption in which proposed standard for computerized marks in view of RSA were presented. A. Curigert portrays VINCI: VLSI Implementation of the new mystery key piece Cipher IDEA. VINCI's IDEA head silicon acknowledgment coordinates rapid encryption and unscrambling, far reaching key administration capacities, what not institutionalized figure methods of operation in their customary and rapid adjusted renditions.

R. Zimmermann et. al. [10] gives a 177 Mb/s VLSI execution of the International Data Encryption Algorithm in which the VLSI chip actualizes information encryption and decoding in a solitary equipment unit. Immeasurably imperative institutionalized methods of operation of piece figures, for example, ECB, CBC, CFB, OFB, and MAC, are bolstered. Additionally, with a framework clock recurrence of 25 MHz the device allows an information change rate of more than 177 Mb/s.

Stefan Wolter [11] gives the IDEA's execution building design that incorporates a simultaneous individual test in view of a mod3 buildup code self-checking framework. It permits the recognition of changeless and transitory single and various piece blunders in the IDEA information way. Thus it gives the protected aversion of flawed scrambled or decoded information. Seung-Jo Han [12] portrays the enhanced DES calculation in which a 96-bit information square is separated into three 32-bit sub-pieces to build the Unicity Distance (UD) by performing distinctive functions on each of the sub-square.

Hassina Guendouz et. al. [13] depicts quick model of a quick information encryption standard with trustworthiness handling for cryptographic applications. It actualizes the DES calculation in the same silicon territory with rapid execution in view of VHDL details K. Wong gives a solitary chip FPGA usage of the Data Encryption Standard (DES) calculation depicting the DES calculation is secured in a solitary chip FPGA by stacking the arrangement information into the chip amid the instatement cycle. When the key is stacked, it is secured inside the chip.

K. Wong [14] performed change area investigation of DES calculation by utilizing instrument. DES can be viewed as Non Linear Feedback Shift Register (NLFSR) with info and for pseudo- irregular succession examination were connected to S-Boxes in DES. They broke down the properties of S-Boxes of DES under diverse changes. They demonstrated that out of 32 capacities from GF(26) to GF(2) connected with eight S-Boxes, around two-third of them had maximal straight compass of 63 and the staying 33% had straight compasses more noteworthy than or equivalent to 57. They have additionally demonstrated that for each of the 32 capacities, broadened hadamard change spectra have the same circulations as that of hadamard change spectra of that capacity.

M.P. Leong [15] portrayed somewhat serial execution of the International Data Encryption Calculation (IDEA) utilizing a novel piece serial building design to perform augmentation modulo 216 by having insignificant measure of equipment. They additionally proposed new criteria that can be considered for the configuration of piece figure calculations: i) bigger straight compass for every segment capacity, ii) the same ghastly conveyance for all broadened Hadamard changes concerning the Hadamard changes.

R. G. Sixel et. al. [16] depicts an abnormal state dialect usage of the DES and bit-cut structural planning. This execution had two targets: (i) testing the entire calculation preceding a VHDL depiction for future amalgamation, and (ii) by making DES accessible for different applications requiring a product usage. Teo Pock Chueng [17] gives execution of pipelined DES utilizing Alter CPLD. The construction modeling contains of three primary parts, DES module, pipeline module and control unit module. Four portions pipeline is utilized as a part of this building design to blast the throughput of DES and Alter Equipment Description Language (AHDL) is utilized to actualize the pipelined DES plan for better yield. It permits element circuit specializations which depend on a particular key and mode. At the point when these are consolidated with a

velocity proficient format, the outcome is a throughput of over 10 Gbits for every second.

Yeong-kanglai et. al. [18] spoke to the VLSI structural engineering outline and execution for two fish square figure. In this paper the two's security fish encryption calculation was expanded by utilizing circle collapsing procedures with effective equipment mapping. Touriaarich gives equipment usage of the information encryption standard in electronic code book mode (ECB) utilizing equipment depiction dialect VHDL.

Toby Schaffer et. al. [19] depicts an incorporated outline of Advanced Encryption Standard (AES). This system is utilized to make it low multifaceted nature structural engineering and aides in sparing the equipment asset in the usage of AES. It is the systems utilizing Random number generator utilizing the repeat lattices and a fourfold vector. It gives information encryption at two levels and subsequently security against crypto investigation is accomplished at moderately low computational overhead utilizing the mod capacity

Cameron Patterson [20] gives superior DES encryption in Vertex FPGAs utilizing Jbits. Jbits gives a Java-based Application Programming Interface (API) for the run-time creation furthermore for the arrangement's adjustment bit-stream. The creator additionally gave an execution examination of information encryption calculations in which different calculations were thought about and it was found that Blowfish calculation is the best calculation in perspective of preparing time and security.

3.Conclusion

In this review paper, we have presented the review for cryptography and DES encryption based FPGA on the basis on the work done in the relevant filed.

References

[1] D. Kahn: The Code breakers: the story of secret writing, MacMillan publishing, 1996.
[2] W. Diffie and M. Hellman, ‐New Directions in Cryptography‖, IEEE Transaction on Information Theory, Vol. IT-22, 1976, pp. 644-654.
[3] Ruth M. Davis, ―The Data Encryption Standard‖, Proceedings of Conference on Computer Security and the Data Encryption Standard, National Bureau of Standards, Gaithersburg, MD, 1977, NBS Special Publication 500-527, pp 5-9.
[4] Whitfleld Diffie, ‐Cryptographic Technology: Fifteen Year Forecast‖ Reprinted by permission AAAS, 1981 from Secure Communications and Asymmetric Crypto Systems. AAAS Selecte8 Symposia. Editor: C.J. Simmons. Vol. 69, West view Press, Boulder, Colorado, pp 38-57.
[5] Ingrid Verbauwhede, ‐Security and Performance Optimization of a New DES Data Encryption Chip‖, IEEE journal of Solid-State Circuits, Vol. 23, No. 3.1988, pp 647-656.
[6] James E. Katz, ‐Social Aspects of Telecommunications Security Policy‖, IEEE journal Technology and Society Magazine, 1990, pp 16-24.
[7] H. Bonnenbergt, VLSI Implementation of a New Block Cipher‖, IEEE journal on Information Theory 1991, pp 510-513.
[8] K.H. Mundt, ‐SUPERCRYPT, ASIC Technology facilitates a new Device Family for Data Encryption‖, IEEE journal on cloud computing 1992, pp 356-359.
[9] C. Boyd. ‐Modern Data Encryption, ‖ Electronics & Communication Engineering Journal on data security and neural networks 1993, Vol. 5, pp 271-278.
[10] R. Zimmermann, ‐A 177 Mb/s VLSI Implementation of the International Data Encryption Algorithm‖, IEEE Journal of Solid-State Circuits. Vol. 29, No. 3, 1994, pp 303-307.
[11] Stefan Wolter ‐On the VLSI Implementation of the International Data encryption Algorithm IDEA‖, IEEE journal on computer system and data security 1995, pp 397-400.
[12] Seung-Jo Han, ‐The Improved Data Encryption Standard (DES) Algorithm IEEE journal on information system 1996, Vol. 3, pp 1310-1314.
[13] Hassina Guendouz, ‐Rapid Prototype of a Fast Data Encryption Standard with Integrity Processing for Cryptographic Applications‖, IEEE transaction on data originations 1998, pp 434-437.
[14] K. Wong, ‐A Single-Chip FPGA Implementation of the Data Encryption Standard (DES) Algorithm, Global Telecommunications Conference, 1998. GLOBECOM 98, IEEE, Vol. 2, pp. 827-832.
[15] M.P. Leong, ‐A Bit-Serial Implementation of the International Data Encryption Algorithm IDEA‖, 2000 IEEE conference Symposium on Field-Programmable Custom Computing Machines, pp 122-131.
[16] R. G. Sixel, ―A High Level Language Implementation of the Data Encryption Standard and a Bit-Slice Architecture‖, Roc 43rd IEEE Midwest Symposium on Circuits and Systems, Lansing MI, 2000, pp 266-269.
[17] Teo Pock Chueng, ‐Implementation of Pipelined Data Encryption Standard (DES) Using Altera CPLD, TENCON 2000 Proceedings, Vol. 3, IEEE 2000, pp 17-21.
[18] Yeong-Kang Lai, ―A Novel VLSI Architecture for a Variable-Length Key, 64-Bit Blowfish Block Cipher, Signal Processing Systems, 1999 IEEE Workshop, pp 568-577.
[19] Toby Schaffer, ‐A Flip-Chip Implementation of the Data Encryption Standard (DES), IEEE1997, pp 13-17.
[20] Cameron Patterson, ‐High Performance DES Encryption in Vertex FPGAs using Jbits, IEEE journal Symposium on FPGA 2000, pp 113-121.
[21] Jingmeiliu, ‐Improved DES Algorithm based on Irrational Numbers, IEEE Int. Conference Neural Networks & Signal Processing Zhenjiang, China, 2008, pp 632-635.
[22] Pui-Lam Siu, ―A Low Power Asynchronous DES, Circuits and Systems, ISCAS 2001 IEEE International conference Symposium, Vol. 4, pp 538-541.
[23] N. Sklavos, ‐Asynchronous Low Power VLSI Implementation of the International Data Encryption Algorithm‖, Electronics Circuits and Systems ICECS

2001, 8th IEEE International Conference Vol. 3, pp 1425-1428.
[24] Ahmet Eskicioglu, Cryptography, IEEE journal on Symposium and Potentials 2001, pp 36-38.
[25] Dragon Jankovi, An Efficient and Scalable VLSI Implementation of DES, ASIC 2001 Proceedings 4th International Conference IEEE on Symposium 2001, pp 341-343.
[26] Massimo Aloito, –Hardware implementations of the Data Encryption Standard‖, IEEE journal on neural networks 2002, pp 100-103.
[27] Chih-Chung Lu, –Integrated Design of AES (Advanced Encryption Standard) Encryptor and Decrypted, Proceedings of the IEEE International Conference on Application- Specific Systems, Architectures, and Processors (ASAP'02).
[28] G. Catalini, –Modified Two fish Algorithm for increasing Security and Efficiency in the Encryption of Video signals, IEEE 2003, pp 525-528.
[29] Aamer Nadeem, –A Performance Comparison of Data Encryption Algorithms, IEEE on Application-Specific Systems, Architectures, and Processors 2005, pp 84-89.
[30] M. McLoone, –High-performance FPGA implementation of DES using a novel method for implementing the key schedule, IEEE Proc.-Circuits Devices Syst., Vol. 150, No. 5, pp 373-378.
[31] William Stallings, ―Cryptography and Network Security Principles and Practices‖, Fourth Edition, 2005, Prentice Hall.
[32] Andrew S. Tanenbaum: –Computer Networks by Prentice Hall.
[33] Jerome Burke John McDonald Todd Austin –Architectural Support for Fast Symmetric- Key Cryptography Advanced Computer Architecture Laboratory
[34] Alan G. Konheim. "Cryptography: A Primer", John Wiley & Sons.
[35] Dominic Welsh, "Codes and Cryptography", Oxford University Press.
[36] Jari Nurmi, "Processor Design: System-On-Chip Computing for ASICs and FPGAs", Springer.
[37] Pong P. Chu "FPGA Prototyping by VHDL Examples: Xilinx Spartan-3 Version", Wiley Interscience.