iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** V **Month of publication:** May 2019

DOI: https://doi.org/10.22214/ijraset.2019.5436

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Performance Analysis of Idea Algorithm on FPGA for Data Security

Pushpalatha G S[1], Harshitha N G[3], Rashmi C[3], Rashmi P K[3], Preksha S[5]
[1]*Assistant Professor,* [2, 3, 4, 5]*Student, Dept. of ECE, Dr. AIT, Bengaluru-560056*

Abstract: ***Data security is important issue in computer networks. Cryptographic algorithms are essential parts in network security. There are plenty of algorithms for the purpose of security. IDEA is one among the proposed algorithm. International Data Encryption Algorithm is symmetric encryption algorithm which is widely used for the purpose of security with simple arithmetic operation. This paper presents an FPGA implementation of IDEA encryption and decryption using Verilog HDL on Spartan 3. It is further implemented for image encryption and decryption using MATLAB. The usage of 128-bit key control makes this algorithm secure and reliable. Experimental synthesis result shows that the proposed design is better where, the delay is reduced to 212.498ns and only 1% of available memory resource is used.***
Keywords: IDEA, Encryption, Decryption, symmetric cipher algorithm, private key, Image encryption.

I. INTRODUCTION

The demand for high security in communication channels, networked instrumentation and distributed measurements and systems is growing rapidly. The confidentiality and security requirements are more important concerns while transmitting and receiving the data. This leads to the need for efficient design of cryptographic algorithms which offers data integrity, authentication, non-repudiation and confidentiality of the encrypted data across the communication channels. Various cryptographic algorithms have been studied and implemented to ensure security of these systems. Single key encryption or conventional encryption in terms that are often used to refer to symmetric encryption. Since symmetric encryption involves usage of private key, it is commonly used than public key encryption. In this paper we represent IDEA algorithm, which is symmetric block cipher encryption algorithm, uses 64 bit plain text, 128 bit key control and produces 64 bit cipher text. Encryption involves 3 major arithmetic operations i.e., Bitwise exclusive OR, Addition modulo 2^{16} and multiplication modulo $2^{16}+1$. Decryption is done in same way as encryption but involves inverse operations. Image encryption and decryption is done for image of size 16X16 using MATLAB.

II. LITERATURE SURVEY

Author Ramesh and Kiran have focused on study of many papers to know which symmetric algorithm is best for implementation. It includes brief description of rounds and operations involved in blowfish, DES, AES, IDEA, CAST-128, RC5.In this survey, classification of algorithms are performed based on different criteria like key-size, encryption or decryption time, throughput, performance, power consumption. Finally it is concluded that AES is better for substantial security, whereas in terms of speed, throughput Blowfish is better and IDEA, RC5, CAST128 are reasonably secure.[1]

Author Rajashekhar, Yong-Bin-Kim and Minsu have proposed implementation of IDEA algorithm on chip designing. It mainly concentrates on $2^{16}+1$ modulo multiplier to decrease the delay in the operation. Compressors are used for system operations where multiplexers are used instead of XOR operations. Key generation process involves Carry Generation blocks, and a spare tree method is used for the final step addition operation. Finally the comparison of performance analysis is given saying that, Encryption rate is improved to 412.15Mb/sec. [2]

Author Thaduri, Gaede and Yoo have proposed the VLSI implementation of IDEA block cipher using VHDL on AMI 0.5 process technology standard cells. Optimization of the modular multiplier design is performed using the temporal parallelism of modules like modulo addition and multiplication. The memory used for the sub-key generated is maintained constant by maintaining the same primary key unless key is changed. It also gives the chip implementation procedure and concludes that the proposed methodology works at 10mhz and the throughput is >700mbps.It is also mentioned that, more enhancement in the modulo multiplier will more increase the performance in the system.[3]

Author Sapna and Ravi mohan have proposed new methodology which reduces time delay, area consumed in existing design. Among the three major operations namely modulo multiplication, modulo addition and XOR, modulo multiplier increases the circuit complexity. Each round has 4 modulo multiplier on critical path. The proposed system divides modulo multiplication into 2 parts: (1) Modulo zero case and (2) Modulo non zero case. Here case (1) is very rare so it is extracted outside critical path, whereas

(2) involves partial product matrix generation which is implemented using carry save adder(CSA) with Wallace structure and summation circuit for partial product matrix implemented using Carry look ahead adder(CLA). Using Xilinx EDA synthesise results shows that delay is reduced to 26.16ns, maximum speed is 37.57 MHz and it is 16% more area efficient and faster than existing design.[4]

Author Sneha and Prof. Vrunda have modified algorithm in which key size is increased from 128 bits to 256 bits, leading to increase in complexity of algorithm. It also uses two multiplicative additive blocks in single rounds rather than one multiplicative additive which increase the diffusion. Instead of 8 rounds as original IDEA algorithm, it is designed for 12 rounds. With all these, the main effort is to increase the cryptographic strength.[5]

Author Osama, Hajar have proposed a system which makes use of 512 bits of key. It is known that IDEA consists of largest weak key and its prone to security attack by adversaries. In order to overcome this, the paper presents solution by increasing key size from 128 bit to 512 bit, thereby increasing the degree of diffusion. Along with this, it uses S-box which reduces the size of block from 32 to 16 bit. This proposed system uses 2 multiplicative additive blocks which strengthen the diffusion. It has told that, it uses total of 104 sub-keys, it strengthen the complexity of confusion which leads to unauthorised attacks. As a result algorithm is more secure and less responsive to cryptanalysis.[6] Author Andreea et. all have discussed about the novel hardware implementation of IDEA NXT encryption algorithm and proposed a strategy for testing the implementation of alter DE2 FPGA. The analysis is performed in terms of execution time, throughput by comparing DES, IDEA and AES algorithm. IDEA NXT family has 2 block cipher with different size, key length and number of rounds; they are I) Standard NXT 64 which is compatible with IDEA and Triple DES. ii) Standard NXT 128 which is compatible with AES. Here Key length is used to choose desired length of password, no of rounds which determines the security of the application. Comparison with respect to both software and hardware implementation is performed to analyse the IDEA NXT. Hence IDEA NXT having high-security is obtained with hardware implementation.[7]

Author Krishna, Lakshmi and Rajani have addressed the encryption techniques AES, RSA, DES and IDEA which can be combined or addressed separately. It is focused on multistage encryption which works in different domain. There are personal domain and public domain. Personal domain makes use of RSA algorithm and DES, whereas AES and IDEA algorithm are used for public domain. Here Data encryption uses public key and Data decryption uses private key. The performance analysis of RSA plus DES, RSA plus AES, RSA plus IDEA is discussed. It is concluded that performance of RSA plus IDEA is very high compared to other cases which takes very less time for encryption compared to other combination.[8] From the above survey, in [1] given that, the algorithm can be implemented on multi-core processors. But currently it is implemented on single core processors. The spare tree method used in [2] has internal limitations which again lead to the drawback of the paper. [4] Though this methodology has higher efficiency, it is not practically implemented yet. In [5], [6] the algorithm makes use of 12 and 16 rounds, which increases complexity there by leading to delay. Since combination of algorithm is used in [8], it again leads to complexity. Thus, the proposed methodology gives complete implementation of encryption and decryption which uses less area, memory, increases speed and efficiency with less delay.

III. IMPLEMENTATION

The paper briefly explains about the encryption and decryption of both text and image using IDEA algorithm. IDEA takes 64 bit plaintext and 128 bit key as input and produces 64 bit of cipher text. Section (I) provides brief description about text encryption and decryption and section (II) for image encryption and decryption.

A. Encryption and Decryption of Plain-Text

The input plain text and key undergoes three operations such as, Data separation, key generation, Encryption and decryption. IDEA totally has 8.5 rounds, in which 8 rounds are performed between plaintext and cipher key and last round is for output transformation. Encryption process is similar to decryption process, but it generates two different types of keys using same 128 bits of key.

1) *Data Separation:* The 64-bit input is divided into four blocks of 16-bit data say, X1, X2, X3, X4. These blocks are given as input to the round 1.
2) *Key Generation:* The 128-bit input key is divided into 8 blocks of 16 bit sub keys. IDEA has 8.5 rounds and requires 52 sub keys for encryption/decryption and each round requires 6 sub-keys of 16 bit. The remaining 2 sub-keys are used in second round; new sub-keys are obtained by circular left shift of 25 bit.
3) *Encryption:* The process consists of eight identical rounds, followed by an output transformation. Each round involves 14 steps as shown in figure1, which are carried out using modulo multiplication, modulo addition and XOR. Out of 52 sub-keys, 48 are used in 8 identical rounds, remaining 4 sub-keys are used in output transformation where 2 inner blocks are swapped and operations are as shown in figure2.After all the operations, obtained cipher text is 64 bit.

4) Decryption: It is done in same way as encryption but involves inverse operations.

The outputs of Text encryption and decryption are shown in figure 3.

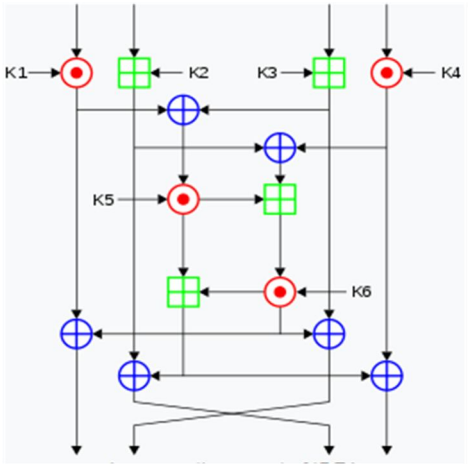


Figure 1.An encryption round of IDEA

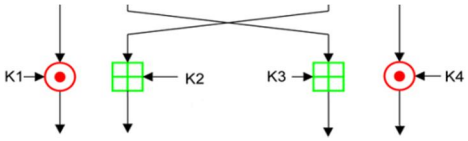


Figure 2.Output transformation process

B. Encryption and Decryption of Image

Image encryption is done using MATLAB R2017a.The colored image of 16x16x3, which exceeds 64 bits. Thus by converting colored image into grey image the size of image is reduced to 16x16(64 bits) as shown in figure 4.

From the grey image16x16 pixel values are extracted. The obtained 256 values are of decimal type. These decimal values are converted into hexadecimal values and they are stored in text file.

The text file generated is given as input to IDEA to get encrypted and decrypted values and are stored in text file format. The obtained encrypted and decrypted images are as shown in figure 5.

The obtained values are reshaped into 16x16 image size to compare encrypted and decrypted images.

IV. RESULTS AND ANALYSIS

To analyse the parameters such as speed, area, delay, memory usage FPGA spartan 3, vertex 5, deviceXC5VLX330T is used. Synthesis is done using XILINX ISE 14.5

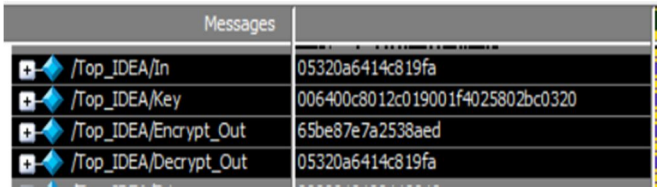


Figure 3. Outputs of text encryption and decryption

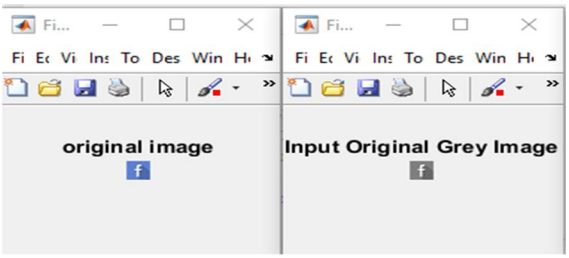


Figure 4. Colored and grey image

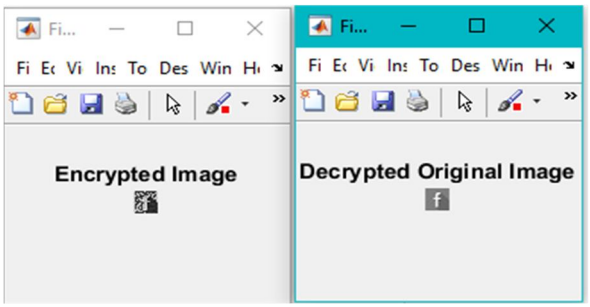


Figure 5. Encrypted and decrypted image

Table 1. Performance Analysis results of IDEA implementation on Xilinx ISE.

Parameters considered	Available Resource	Used resource	Utilization (in %)
No of slice LUTs	2,07,360	2,720	1%
No of bonded IOBs	960	320	33%
No of occupied slices	51,840	808	1%

The table.1 shows the result of performance analysis. The total delay timeis reduced to 212.498ns or 0.21us (176.152ns logic, 36.347ns route). Total REAL time and CPU time for Xst completion are 57.00 secs and 57.24 secs respectively. Total memory usage is 798280 kilobytes.

Table 2. Comparison of different design for evaluating delay and area.

Design	Delay	Area (Resource used)
Cheung[11]	2.134us	79.56% (XCV300)
Thaduri[3]	0.8us	1.95mm^2(EPF10K70 RC240)
Hamalainen[12]	1.246us	65% (XCV100E-6)
Rahul[13]	0.27us	1.54mm^2 (ASIC)

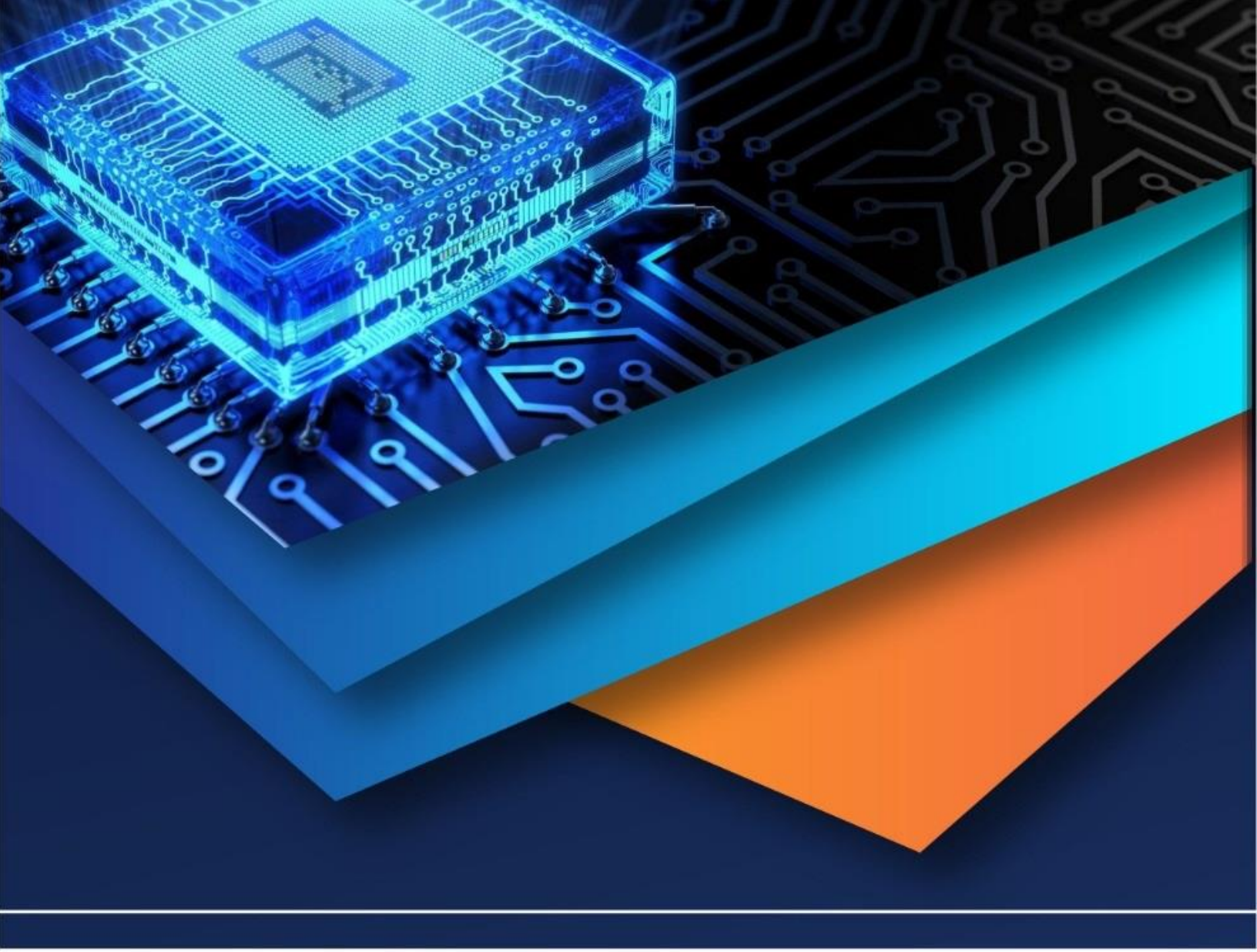
The above table 2 shows comparison of various parameters such as area, delay after implementing design on hardware.

V. CONCLUSION AND FUTURE SCOPE

The importance of protecting data from adversaries and hackers is increasing day by day. This paper presents efficient implementation of IDEA on hardware. The delay is reduced to 0.21us and only 1% of memory is utilized.
Further this design can be implemented on multi-core processors for enhancing speed, efficiency and delay performance.

REFERENCES

[1] Ramesh, R. Kiran. 2016. A survey on Conventional encryption algorithms of cryptography, IEEE.
[2] Rajashekhar, Yong-Bin-Kim and Minsu Choi. 2010. Design and performance measurement of efficient IDEA crypto-hardware using novel modular arithmetic components, IEEE.
[3] M. Thaduri, S. -M.Yoo, R. Gaede. 2004. An efficient VLSI implementation of IDEA encryption algorithm using VHDL, Elsevier.
[4] Sapna, Ravimohan. 2014. An improved and fast design of IDEA encryption on FPGA, IJSETR.
[5] Ms Snehal Patil, Prof.Vrunda Bhusari.2014. An Enhancement in International Data Encryption Algorithm for Increasing Security. IJAIEM
[6] Osama Almasri, Hajar Mat Jani. 2013. Introducing an encryption algorithm based on IDEA, IJSR.
[7] Andreea, Flavius, Mircea. 2013. Hardware Implementation of IDEA crypto- algorithm, IEEE.
[8] Krishna, Lakshmi, Rajani. 2017. Performance analysis of various Encryption algorithms for usage in Multistage encryption for securing data, IEEE.
[9] Lai. X, Massey. J. 1990. A proposal for a new block encryption standard, Eurocrypt'90.
[10] M. Bahrami, B. Sadeghiyan. 2000. Efficient modulo 2n+1 multiplication scheme for IDEA, IEEE.
[11] Cheung, Tsoi, Leong. 2001. "Tradeoffs in implementation of IDEA", Springer.
[12] Hamalainen, Tomminska.2002. "6.78Gbps implementation of IDEA", ICFPLA.
[13] Ranjan, Rahul. 2008. "VLSI implementation of IDEA using VHDL", Microprocessors and Microsystems 29.1



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY