International Journal of Advanced and Innovative Research (2278-7844) /
Volume 7 Issue 2

Design and Verification of ASIP- Dual Modified Key Generator Based Encryption for Cloud Storage

Astha tiwari, GGITS, Jabalpur
Prof. Muhammad Arif, GGITS, Jabalpur

Abstract: Paper work proposed a new 2^n+1 modulo multiplier for dual key IDEA encryption in the design which generates less number of partial products (≤ n 2) and the less area at very high speed. The multiplication is based on Wallace tree along with specialized shifting. Coding with different combinations of eight rounds is been done at gate level i.e. fully dataflow modeling style for high throughput.. New modulo multiplication is been proposed in which multiple patterns can be done with less area. The string matching module is coded and functionally verified using VHDL language targeting Virtex IV pro FPGA and performance measures in terms of speed and resource utilization. Our work is mainly based on designing an efficient architecture (IP) for a cryptographic module for secure data trafficking and a network intrusion detection system for a high speed network. The complete designs are coded using VHDL language and are verified using Xilinx-ISE simulator for verifying their functionality.

Keywords: Advance encryption System (AES) , Integrated Simulation Environment (ISE) ,Field Programmable Gate Array (FPGA) , Corrected Block Tiny Encryption Algorithm (XXTEA), International data encryption algorithm (IDEA) , Secured and fast encryption routine (SAFAR) , Network Intrusion Detection System (NIDS)

I-INTRODUCTION

International Data Encryption Algorithm (IDEA) is a block cipher technique designed by Mr. Xuejia Lai and James L. Massey [7] of ETH-Zurich and was first introduce in 1991. It is a modified version of an earlier cipher, PES (Proposed Encryption Standard); Dual key IDEA was known as at initially IPES (Improved PES). Dual key IDEA was used as the symmetric dual key cryptography in initial version of the Pretty Good Privacy cryptosystem (PGPC). Dual key IDEA was to develop as a strong encryption algorithm, which could replace the DES procedure developed in the U.S.A. in the seventies data transfer. It is also good to know that it fully avoids the use of any lookup tables or Substitution-boxes (SBOX). The famous PGP email and file encryption product was designed by Phil Zimmermann, uses Dual key IDEA as their original choice for data encryption based for its proven design and its well reputation. Cryptography is method for secure data communication while it is not a compulsory requirement of data communication because data communication can be done without Encryption or decryption but because of intruders it became essential for modern data communication, as it is not a compulsory part of data communication so it is simply a overhead and some time that encryption is very complex so it requires very high computation and huge area requirement and also need lots of time to generate the cipher which overall reduce the throughput of data communication, and in modern communication the high speed data communication is one of major requirement by the data users.

The available Encryption methods like AES, DES, Blowfish, and RSA etc. are good enough but require lots of time and area and power requirement like for this a new encryption method is been developed and presented in the thesis work which is highly secure (highly avalanche) , highly throughput (less computation time) as compare existing encryption methods.

II-METHODOLOGY

The paper work is an new approach in the encryption area, the motivation behind the work is that Encryption and decryption is an very important requirement now a days but it is not the compulsory requirement for the data communication it is just a important need, the work done in the area till now is itself an achievement and very robust, but it is also an overhead for the system and the hardware and time requires for the encryption and decryption is just a overhead for the system, proposed work is an highly secure encryption techniques for data communication with less amount of hardware and less time, the proposed work is the encryption technique which is less complicated and uses proposed new unique transform encoding..

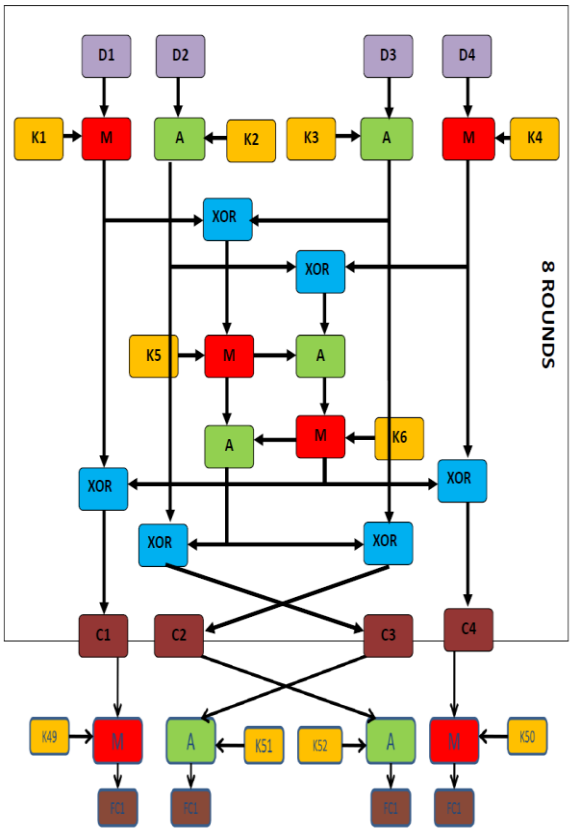

Figure 1 International Data Encryption Algorithm (IDEA)

Figure 2 above shows working flow of IDEA cipher encryption here M is modulo multiplier, 'A' is modulo adder K1-K6 are 16 bit part to Key. In each round to 8 rounds to algorithm, following sequences to events [7] are performed:

1. modulo Multiply D1 & K1
2. Modulo Add D2 & K2
3. Modulo Add D3 & K3
4. modulo Multiply D4 & K4
5. XOR results to step 1 & step 3
6. XOR results to step 2 & step 4
7. Modulo Multiply results to step 5 with K5
8. Modulo Add results to step 6 & step 7
9. Modulo Multiply results to step 8 with K6
10. Modulo Add results to step 7 & step 9
11. XOR results to step 1 & step 9
12. XOR results to step 3 & step 9
13. XOR results to step 2 & step 10
14. XOR results to step 4 & step 10

Key generation:

Original Key= K8 K7 K6 K5 K4 K3 K2 K1
Rotate left by 25 bit= K16 K15 K14 K13 K12 K11 K10 K9
Rotate left by 25 bit =K24 K23 K22 K21 K20 K19 K18 K17
Rotate left by 25 bit =K32 K31 K30 K29 K28 K27 K26 K25
Rotate left by 25 bit =K40 K39 K38 K37 K36 K35 K34 K33
Rotate left by 25 bit =K48 K47 K46 K45 K44 K43 K42 K41
Rotate left by 25 bit =K56 K55 K54 K53 K52 K51 K50 K49

K1-K6 to round two
K7-K12 to round three
K13-K18 to round four
K19-K24 to round five
K25-K30 to round six
K31-K36 to round seven
K37-K42 to round eight
K43-K48 to round nine
K49-K52 to round ten

Each to eight complete rounds necessary six sub keys & final transformation "half round" necessary four sub keys. So entire procedure necessary 52 sub keys. 128-bit key is split into eight 16-bit sub keys. Then bits are shifted to left 25 bits. Resulting 128-bit string is split into eight 16-bit blocks that become next eight sub keys. Shifting & splitting procedure is repeated until 52 sub keys are generated. Shifts to 25 bits ensure that repetition does not occur in sub keys. Six sub keys are used in each to 8 rounds. Final 4 sub keys are used in ninth "half round" final transformation. Six 16-bit key sub-blocks from 128-bit key. Since a further four 16-bit key-sub-blocks are required to subsequent output transformation, a total to 52 (= 8 x 6 + 4).

First, 128-bit key is partitioned into eight 16-bit sub-blocks which are then directly used as first eight key sub-blocks.
The 128-bit key is then cyclically shifted to left by 25 positions, after which resulting 128-bit block is again partitioned into eight 16-bit sub-blocks to be directly used as next eight key sub-blocks.
The cyclic shift procedure described above is repeated until all to require 52 16-bit key sub-blocks have been generated.

Proposed Modulo Multiplier: As observed from the Dual key IDEA cipher algorithm there is four types of computation $(2^n + 1)$ modulo multiplier, (2^n) modulo adder, XOR and shifter in key generation. Out of these the ability to perform fast modulo 2^n+1 multiplication is then still a major challenge, particularly from a hardware point of view. Even though a modulo $2^n + 1$ multiplier can be implemented using look-up tables, the memory requirements are a big constraint for large values of *n*. Hence, to avoid the exponential growth of the memory requirements several implementations based on combinational arithmetic circuits have been proposed. Figure 2 below explains the working.

First let for n=4

$(2^n + 1)$ can be factorized in four forms below:-

R1=10001000
R2=01000100
R3=00100010
R4=00010001

R1, R2, R3 and R4 are possible four various factors of 2^4+1

Let if X=0110 and Y= 0101
Than XY = 011110

Possible solution with proposed method is =>
00011110 – 00010001 => 0000111

Observed ANS in only one step
Let if X=1110 and Y= 1101
Than XY= 10110110

Possible solution with proposed method is =>
10110110 – 10001000 => 00101110 - 00100010 => 00001100

Observed ANS in only two steps
Let if X=1010 and Y= 1101
Than XY= 10000010

Possible solution with proposed method is =>
10000010 – 01000100 => 00111110 - 00100010 => 00011100-00010001=>00001001

Observed ANS only in three steps it is MAX steps required with proposed architecture

The same approach is been used for 2^8+1 and $2^{16}+1$ modulo multiplier. Figures of Proposed $(2^n + 1)$ architecture are shown in figures next pages for n=4

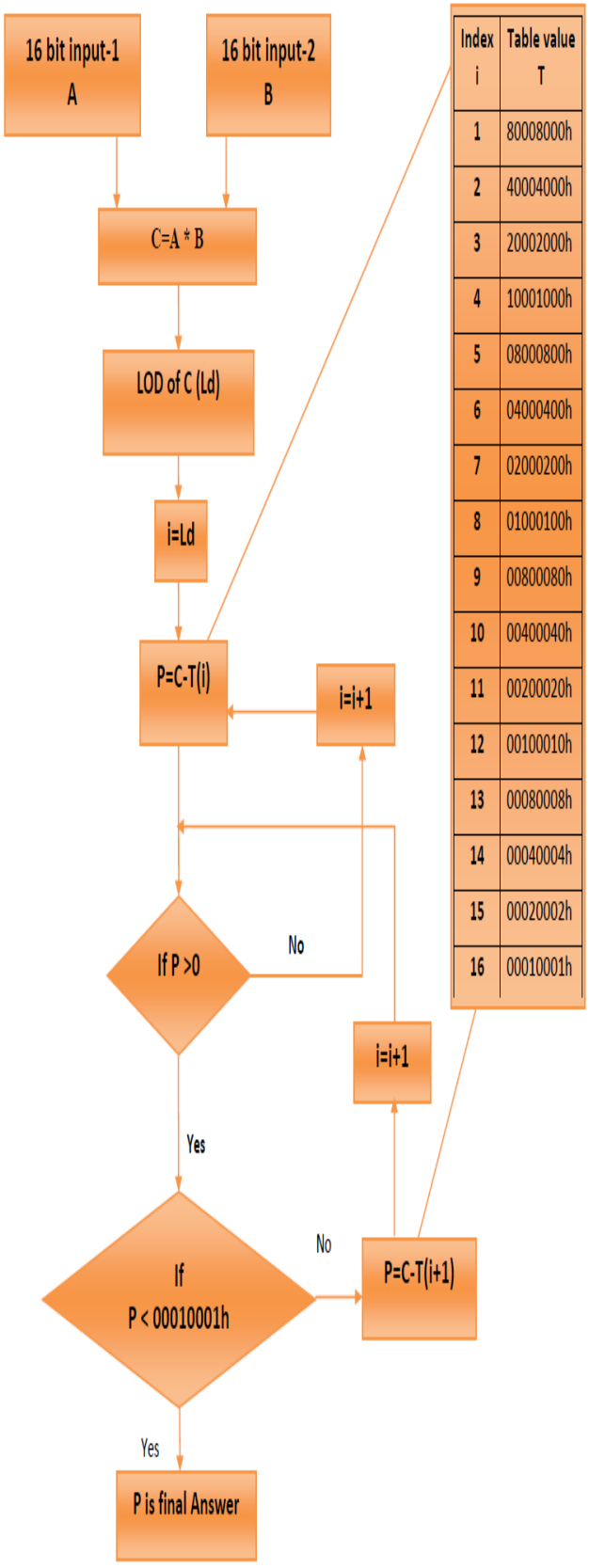

Figure 2 Proposed new modulo $(2^{16}+1)$ Multiplier

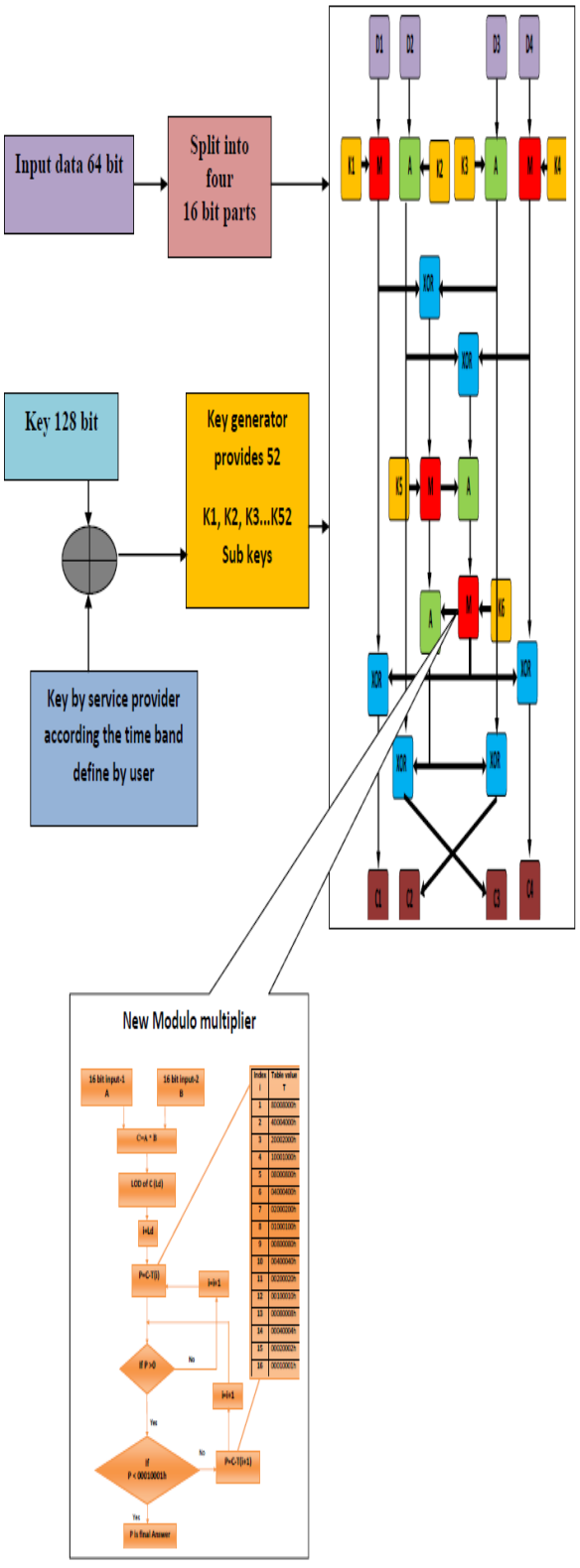

Figure 3 Block diagram of proposed work

Figure 3 shown above is the overall working of proposed work here the size of initial data is of 64 bit then there is One single 128 bit Key1 provided by user and one 128 bit Key2 provided by service provider which will be based on the time of encryption and tentative time of decryption Final KEY is XOR of Key1 and Key2 With the help of final KEY and Key-generator 52 sub-keys developed as k1, k2, k3.....k52. Proposed work did all this for dual key based security which simply squared the encryption security.

After all that this keys and data provided to IDEA encryption engine which developed the 64 bit output cipher , but there is one change that the modulo multiplier in IDEA encryption engine is new proposed by us, and this new modulo multiplier will helps to reduce overall area and enhance the speed of cipher generation.

III-RESULTS

Area: the area in any digital design always required to be reduce as much as possible because area directly related to the overall cost of the system, size of the system, power of the system and as we know power matters in all battery based devices. In FPGA implementation number of slices represents area.

Time delay/ Max Frequency: Time delay or Maximum frequency another important parameters in VLSI deigns because any system performance mainly measure in terms of speed and if it is fast enough that system will consider better.

NEW Project Status			
Project File:	new.ise	Current State:	Synthesized
Module Name:	full	• Errors:	No Errors
Target Device:	xc4vlx200-11ff1513	• Warnings:	39 Warnings
Product Version:	ISE 9.2i	• Updated:	Tue Feb 21 00:31:22 2017

NEW Partition Summary
No partition information was found.

Device Utilization Summary (estimated values)			
Logic Utilization	Used	Available	Utilization
Number of Slices	10273	89088	11%
Number of 4 input LUTs	19448	178176	10%
Number of bonded IOBs	256	960	26%
Number of DSP48s	34	96	35%

Detailed Reports					
Report Name	Status	Generated	Errors	Warnings	Infos
Synthesis Report	Current	Tue Feb 21 00:31:17 2017	0	39 Warnings	0
Translation Report					
Map Report					
Place and Route Report					

Figure 4 Synthesis results

Figure 4shows the synthesis results and register transfer level (RTL) results of the proposed design. Table below represents synthesis results

Target device Vertex 4 VLX200 FPGA	
Parameters	**Results**
Slices	10273
LUT	19448
IOB	256
Time delay	891.770 ns
Max Freq.	1.1213 Mhz

Table 1 Results obtained

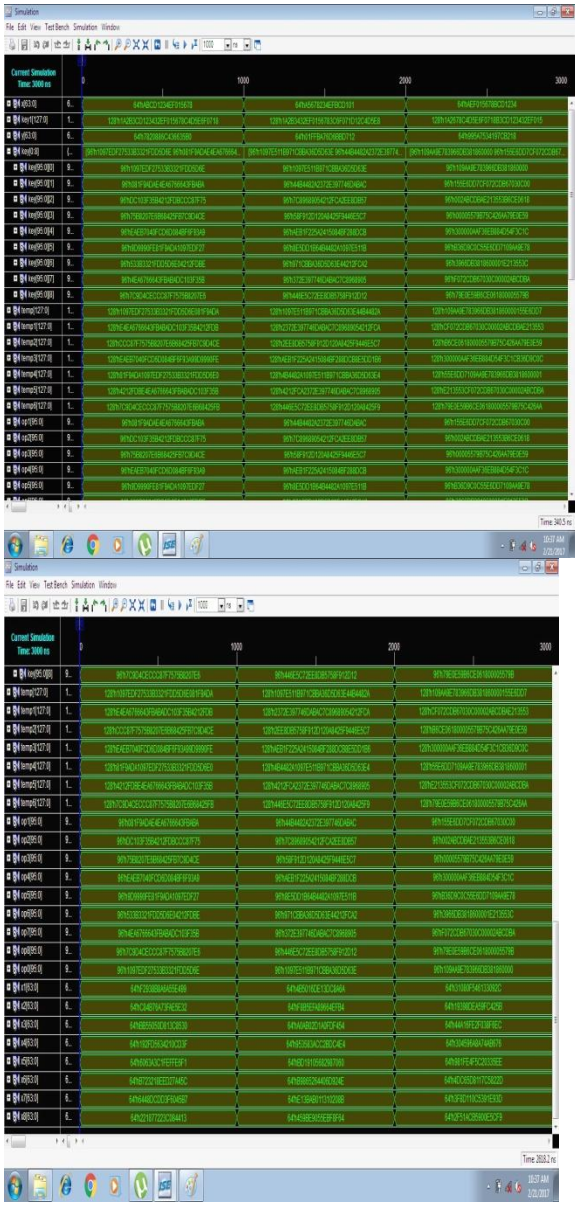

Figure 5 Simulation Results

Figure 5 above shows the simulation results where we can observe the output for three deferent Keys, and different inputs. In simulation we can observe inputs and output after each rounds and also we can observe he process of Key generation and key to each round for all three cases.

Comparative results:

	Slices
Proposed	10273
Zhongyuan Hao [1]	11342
LI Wei [2]	11589

Table 2 Area comparison

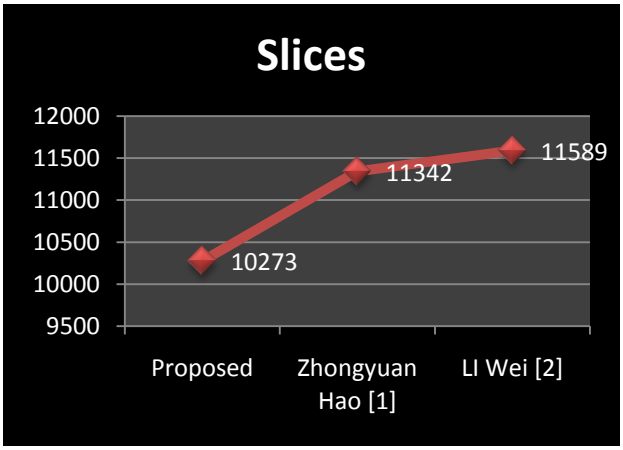

Figure 6 Area comparison

From the table 2 and figure 6 it can be clearly observe that proposed work requires less area as compare with other works.

	Max Freq (Mhz)
Proposed	1.1213
Zhongyuan Hao [1]	1.06
LI Wei [2]	0.982

Table 3 Speed Comparison

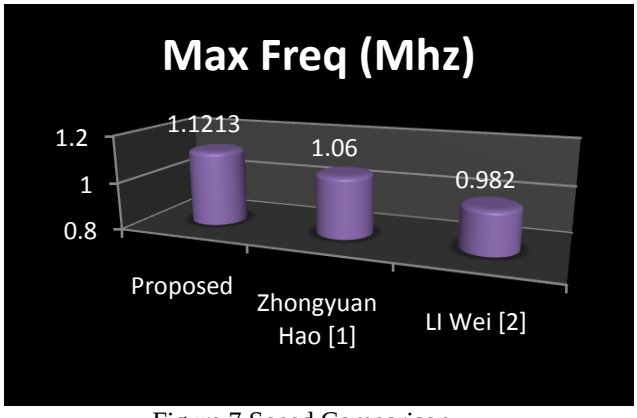

Figure 7 Speed Comparison

From the table 3 and figure 7 it can be clearly observe that proposed work requires less area as compare with other works.

IV-CONCLUSION

Dual key IDEA is a patented and universally applicable block encryption algorithm, which permits the effective protection of transmitted and stored data against unauthorized access by third parties. With a key of 128 bits in length, Dual key IDEA is far more secure than the widely known DES based on a 56-bit key. The fundamental criteria for the development of Dual key IDEA were military strength for all security requirements and easy hardware and software implementation. The algorithm is used worldwide in various banking and industry applications. They predestine the algorithm for use in a great number of commercial applications. Thesis work can finally conclude that the speed of proposed Dual key IDEA cipher generator module is better that previous work done that are discuss in literature review, when area concerns proposed work is moderate.

REFERENCES

[1] Zhongyuan Hao, Wei Guo, Jizeng Wei, Dual Processing Engine Architecture to Speed Up Optimal Ate Pairing on FPGA Platform, 2016 IEEE/Trustcom/BigDataSE/ISPA, DOI: 10.1109/ TrustCom.2016.0113, ISSN: 2324-9013

[2] LI Wei , ZENG Xiaoyang , NAN Longmei , CHEN Tao , DAI Zibin , A reconfigurable block cryptographic processor based on VLIW architecture, China Communications (Volume: 13, Issue: 1, Jan. 2016), DOI: 10.1109/CC.2016. 7405707, Page(s): 91 – 99, ISSN: 1673-5447

[3] Based on the character of cloud storage string encryption and cipher text retrieval of string research, 2016 4th International Conference on Cloud Computing and Intelligence Systems (CCIS), DOI: 10.1109/CCIS.2016.7790293

[4] International Data Encryption Algorithm, swiss encryption technology, and the IDEA logo are trademarks of MediaCrypt AG, Switzerland, Patent protection EU: 0 482 154 B1

[5] Harivans Pratap Singh, Shweta Verma, Shailendra Mishra, Secure-International Data Encryption Algorithm, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Issue 2, February 2013, ISSN (Online): 2278 – 8875

[6] NICK HOFFMAN, A SIMPLIFIED IDEA ALGORITHM, online documents, http://citeseerx.ist. psu.edu/viewdoc/download?doi=10.1.1.501.2662&rep= rep1&type=pdf

[7] Sandipan Basu, INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA) – A TYPICAL ILLUSTRATION, Volume 2, No. 7, July 2011 Journal of Global Research in Computer Science REVIEW ARTICLE Available Online at www.jgrcs.info, JGRCS 2010

[8] Oleg Vyshnyvetshkey, sebistian gulloex, IDEA block cipher final presentation, RIT cryptographic course, 2012

[9] Wikipedia documents, https://en.wikipedia.org /wiki/International_Data_ Encryption_Algorithm

[10] Xilinx documents, https://www.xilinx.com /products/design-tools/ise-design-suite.html

[11] Vertex 4 VLX 200 FPGA datasheet, https://www.xilinx.com/support/documentation / data _sheets /ds112.pdf

[12] NPTL lectures on VHDL, http://nptel.ac.in/courses/117108040

[13] Shihai Zhu, Hardware Implementation of AES Encryption and Decryption System
Based on FPGA Send Orders for Reprints to reprints@benthamscience.ae, The Open Cybernetics & Systemic Journal, 2015, 9, 1373-1377 1373

[14] Swapna kumari , Dasari. Subbarao, Implementation of AES-256 Encryption Algorithm on FPGA, International Journal of Emerging Engineering Research and Technology Volume 3, Issue 4, April 2015, PP 104-108 ISSN 2349-4395 (Print) & ISSN 2349-4409, International Journal of Emerging Engineering Research and Technology V3 I4, April 2015 104