www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 5 May 2016, Page No. 16652-16657

Implementation and Analysis of Multi-Processing Processor Using Data Encryption Standard on FPGA

Soumya D[1], Dr. K Ramesha[2] and Guruprasad S P[3]

PG Student[1]
Dept. of ECE (VLSI & ES)
Dr. Ambedkar Institute of Technology
Bengaluru-56,India
soumyad096@gmail.com

Professor[2]
Dept. of ECE
Dr. Ambedkar Institute of Technology
Bengaluru-56, India
kramesha13@gmail.com

Senior Design Engineer[3]
Certitude Technologies Pvt Ltd
Bengaluru-38, India
guruprasad.sp@vedlabs.com

Abstract: ***The network communication is mandatory and critical in our day-to-day life. The cryptography is the technique to secure the data in communication field such that privacy of data is maintained. The cryptography has different types of algorithms; they are Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Ron Rivest Adi Shamir & Leonard Adlemen (RSA) Triple Data Encryption Standard algorithm (TDES). The Multi-processor is most used in this era as it is subject to constraints while computing. The Multi-processing is the processing of multiple tasks at a time using two or more central processing units in one system. Here in this paper the Multiprocessing processor and light-weight DES algorithm is implemented using Xilinx 14.7. The simulation is done in Model Sim 6.3 and verifying the code is done by dumping onto Spartan 3 Field programmable gate array (FPGA).***

Keywords: Cryptography, DES, FPGA, Light-Weight Processor (LWP), Multiprocessing, Verilog.

1. Introduction

The most tedious part in today's world is Network Communication. Communication is the process of exchanging the information between people or computing systems etc. through some medium.

So the data communicated is secured by means of Cryptography. The Cryptography is the process of hiding the information or converting the information into another form while transferring through some medium.

The Cryptography consists of different algorithms, which convert the transferring data to another form of data and it will be transmitted from one end to another. Different algorithms are Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Ron Rivest Adi Shamir & Leonard Adlemen (RSA).

The Data Encryption Standard (DES) is developed by National Institute of Standards and Technology (NIST). It is frequently used and is easy to understand, because algorithm is applied to block size of 64-bits of data at a time.

The Advanced Encryption Standard (AES) is also developed by NIST and has been approved and adopted by the U.S. government. It is applied to block of 128 bits, with three different key lengths like 128, 192 and 256-bits.

The RSA is one of the first practically implemented public - key cryptographic algorithms. RSA is relatively slow algorithm and uses different keys at transmission side and receiving side.

Multi-processor is widely used in Real Time Operating System (RTOS). It consists of multiple CPU's that are embedded onto one system. The FPGA is an integrated circuit and it is configurable according to customer specification outside the fabrication foundry.

This paper consists of understanding the DES algorithm and implementing the same on Multi-processing processor. In DES the Rounding flow and Key scheduling flow is explained. The results for DES algorithm, Multi-processing processor and DES on Multi-processing processor are analyzed.

2. Related work

The ref. [1] is explaining about design and implementation of DES algorithm. A FPGA based hardware design for Cryptanalysis of DES based on known-plaintext attack using Brute force technique. Two Architectures viz. Iterative and Loop unrolled DES Architecture are implemented.

Iterative architecture requires less area and can search the Entire solution space in less time as compared to the Loop Unrolled architecture. Unrolled architecture consumes more area. The design to fit maximum instances of the key search engine in a single FPGA is more complex.

The ref. [2] paper is speaking about Performance Analysis of Data Encryption Algorithm This provides the performance Comparison between four of the most commonly used Encryption algorithms: DES (Data Encryption Standard), 3DES (Triple DES), BLOWFISH and AES (Rijndael). The Comparison has been conducted by running several setting to Process different sizes of data blocks to evaluate the algorithms Encryption and Decryption speed. Though having so many advantages and application it is still suffered from the Weak Key problem which yet to be rectified and explored.

The ref. [3] is demonstrating the Implementation of Non-Pipelined and Pipelined Data Encryption Standard (DES) Using Xilinx Virtex-6 FPGA Technology. The most commonly used symmetric encryption algorithm, Data Encryption Standard (DES).The VHDL programming is done for the design. The Maximum clock frequency and throughput are provided by DES algorithm. The pipelined architecture has fewer throughputs.

3. Multi-processing light weight processor

The Multi-processing processor handles two or more computations at a time using many central processing units. Multi-processors have been widely used in modern world of high performance embedded system to meet the computational needs of smart and real time applications spread across multiple fields.

The custom IPs (Intellectual Property) on FPGA based systems are commonly used, multiprocessing on FPGAs have not been so much explored due to concerns in meeting a right trade-off between area, speed, throughput and the required design time. This Multi-processing can be modeled into Light-weight processor by means of keeping single central processing unit with multiple threads.

The soft LWP is shown in Figure 1 and consists of five main building blocks. They are: instruction memory, instruction fetch, instruction decode and execution logic. This also includes register file to store the data and used as cache memory for the processor. The execution logic includes DES algorithm which works using Electronic Code Book (ECB) mode.

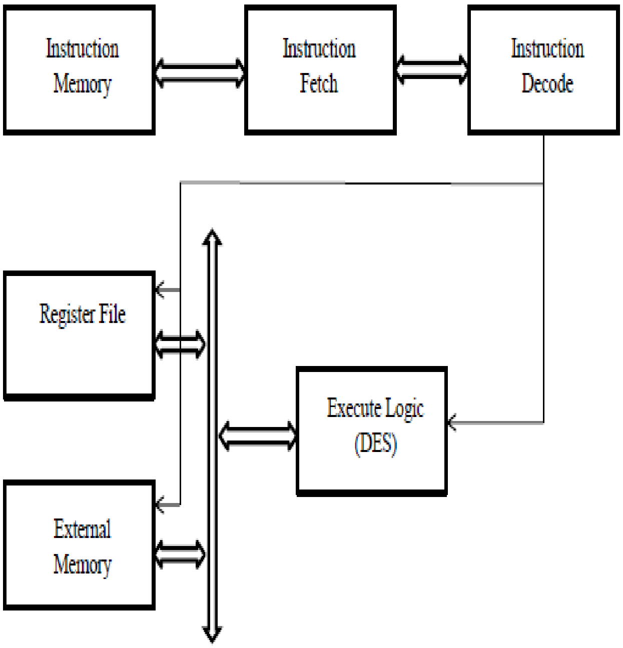

Figure 1: Block Diagram of LWP with DES

The LWP is a pipelined Reduced Instruction Set Computing (RISC) processor. RISC is a type of microprocessor (µp) architecture that uses smaller number of types of computer instructions and highly-optimized set of instructions, than a highly specialized set of instructions. So it will operate at a higher speed that is performing more millions of instructions per second or MIPS.

4. Implementation of DES Algorithm

The Data Encryption Standard (DES) algorithm is one type of symmetric key block cipher in Cryptography.

The DES algorithm is designed by researchers at IBM and is modified by government agencies, the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST). The American National Standards Institute (ANSI) is using DES algorithm as the federal standard for encryption and decryption of commercial and sensitive data. This is described in Federal Information Processing Standards (FIPS 46, 1977) published by NIST.[4]

The DES algorithm is a round Feistel structure with 16 rounds. The input data block is of 64-bits and the key size is 64-bits. After Key Scheduling the key length becomes 48-bits which is an efficient and is used in this algorithm.

The conventional flow of the DES is as shown in Figure 2. The block of 64-bits of data which has to be encrypted is first given to Initial Permutation (**IP**). This is the process of changing the bit positions or rearranging the bit values.ref.[5] The performance of **f** function is in Figure 3. The Key Scheduling is also a round structure of 16 rounds that has left shift and two permutation choices that is shown in Figure 4. The key scheduling algorithm produces 16 different keys with 48-bits size for DES algorithm to process block of data at 16 different rounds and finally the Initial Permutation (**IP**$^{-}$

^{1}) step gives out the encrypted that is cipher text is the output.

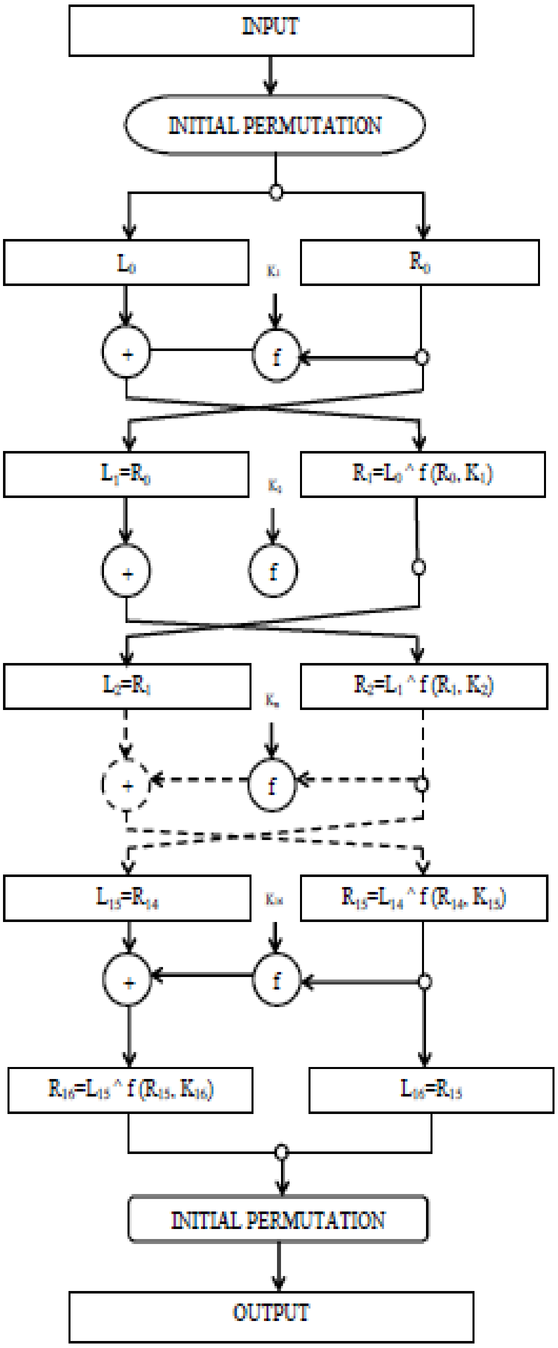

Figure 2: Flow Chart for DES

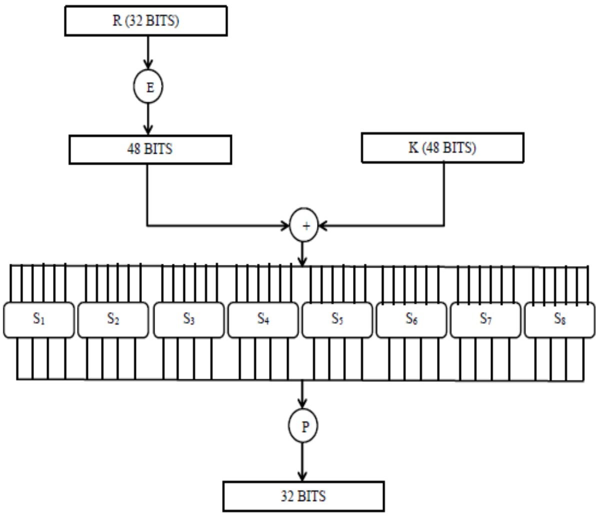

Figure 3: Block diagram of function f(R, K)

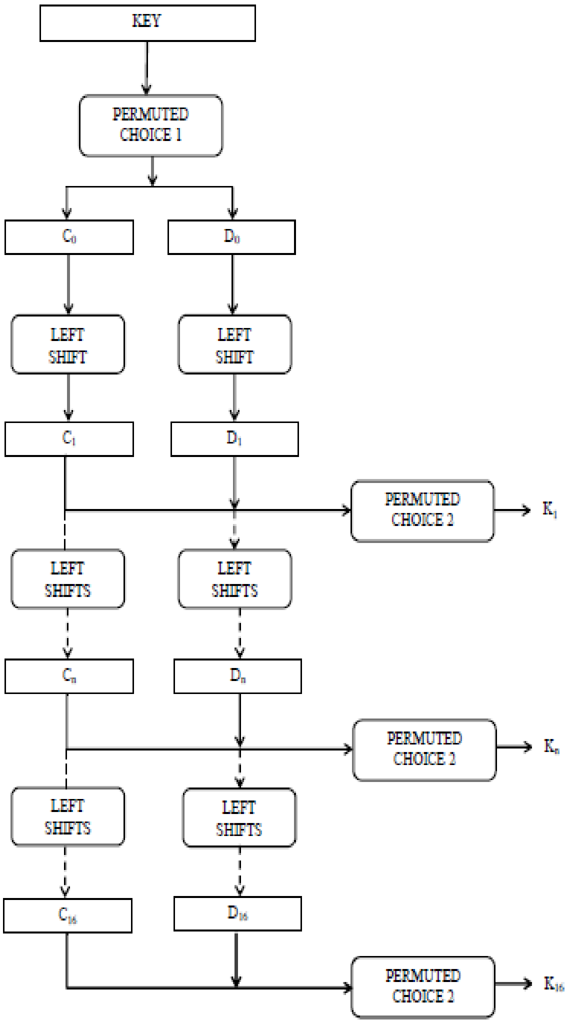

Figure 4: Flow Chart for Key Scheduling

The Decryption is implemented in the invers order that is, keys are sent in the reverse order. The cipher text is the encrypted block of data and the decipher text is the decrypted block of data which is same as plain text.

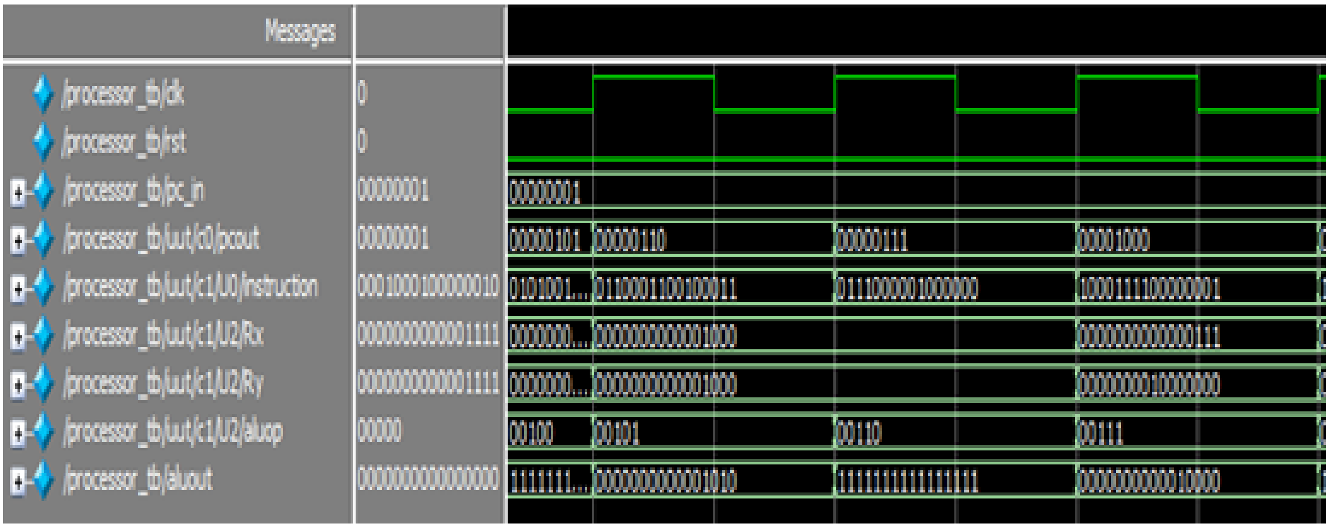

Figure 5: Simulation of Multi-processing processor

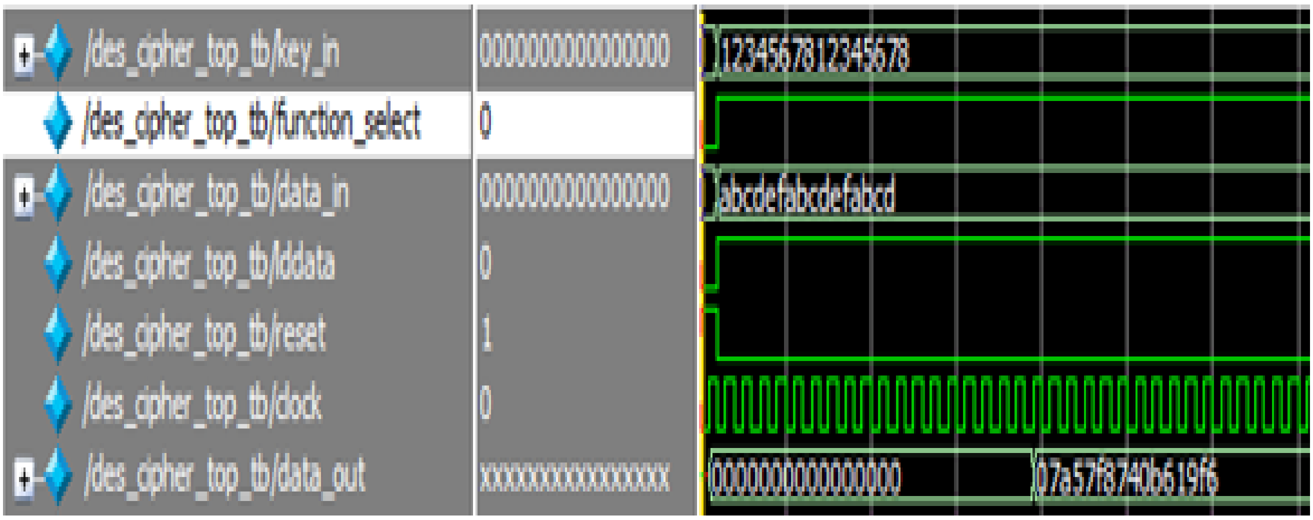
/des_cipher_top_tb/key_in 0000000000000000
/des_cipher_top_tb/function_select 0
/des_cipher_top_tb/data_in 0000000000000000
/des_cipher_top_tb/lddata 0
/des_cipher_top_tb/reset 1
/des_cipher_top_tb/clock 0
/des_cipher_top_tb/data_out XXXXXXXXXXXXXXXX
1234567812345678
abcdefabcdefabcd
0000000000000000
07a57f8740b619f6

Figure 6: Simulation of DES encryption

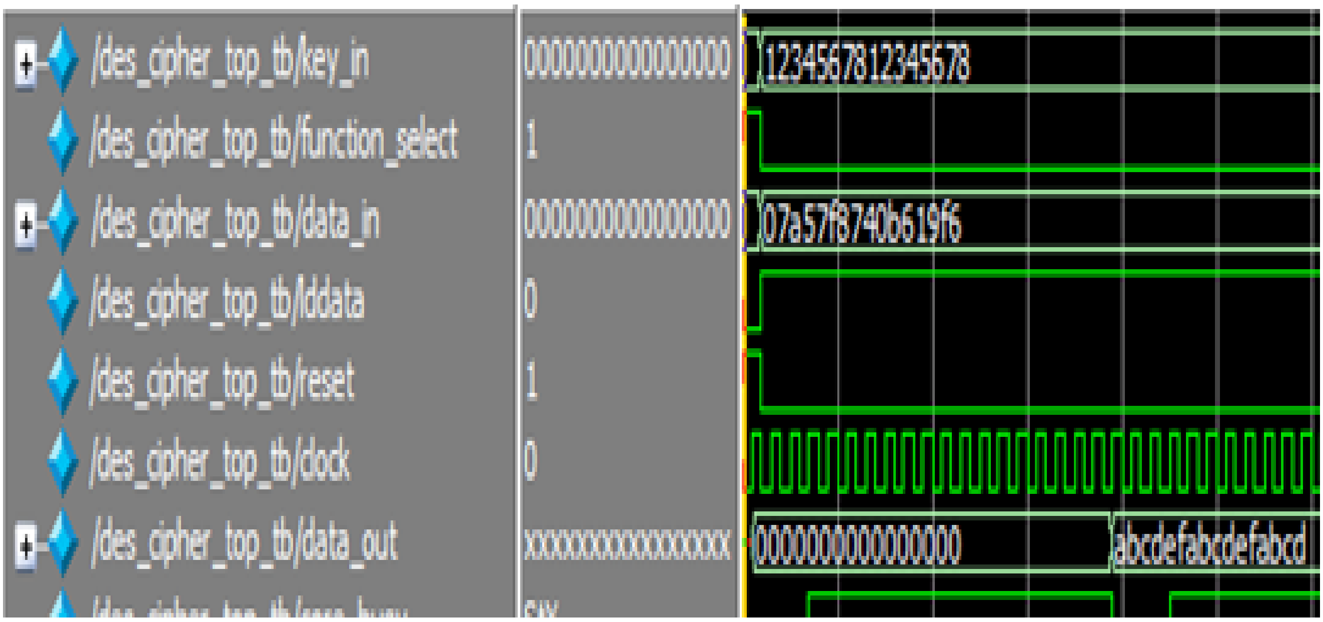
/des_cipher_top_tb/key_in 0000000000000000
/des_cipher_top_tb/function_select 1
/des_cipher_top_tb/data_in 0000000000000000
/des_cipher_top_tb/lddata 0
/des_cipher_top_tb/reset 1
/des_cipher_top_tb/clock 0
/des_cipher_top_tb/data_out XXXXXXXXXXXXXXXX
1234567812345678
07a57f8740b619f6
0000000000000000
abcdefabcdefabcd

Figure 7: Simulation of DES decryption

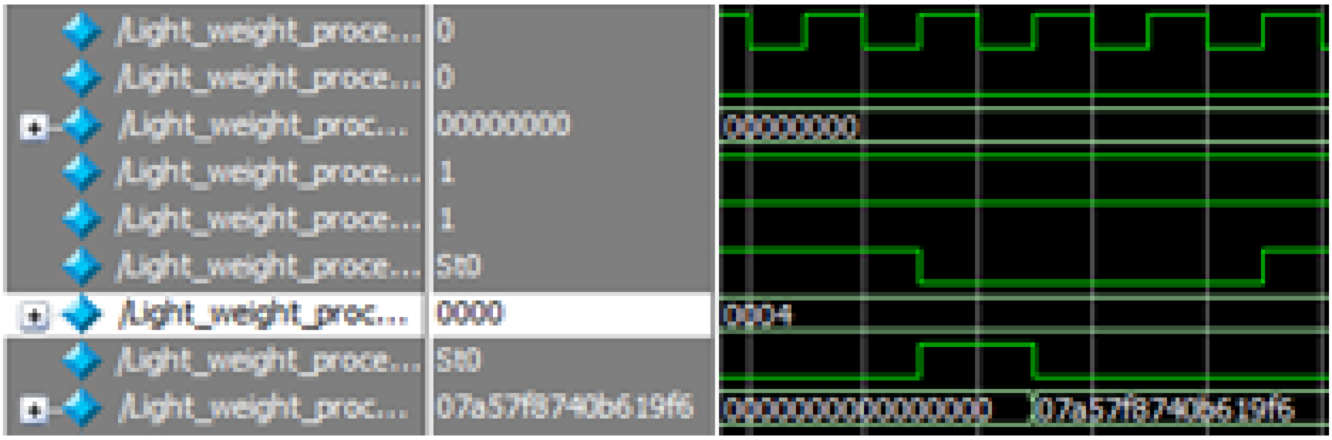
/Light_weight_proce... 0
/Light_weight_proce... 0
/Light_weight_proc... 00000000
/Light_weight_proce... 1
/Light_weight_proce... 1
/Light_weight_proce... St0
/Light_weight_proc... 0000
/Light_weight_proce... St0
/Light_weight_proc... 07a57f8740b619f6
00000000
0004
0000000000000000
07a57f8740b619f6

Figure 8: Simulation of DES encryption on Multi-processing processor

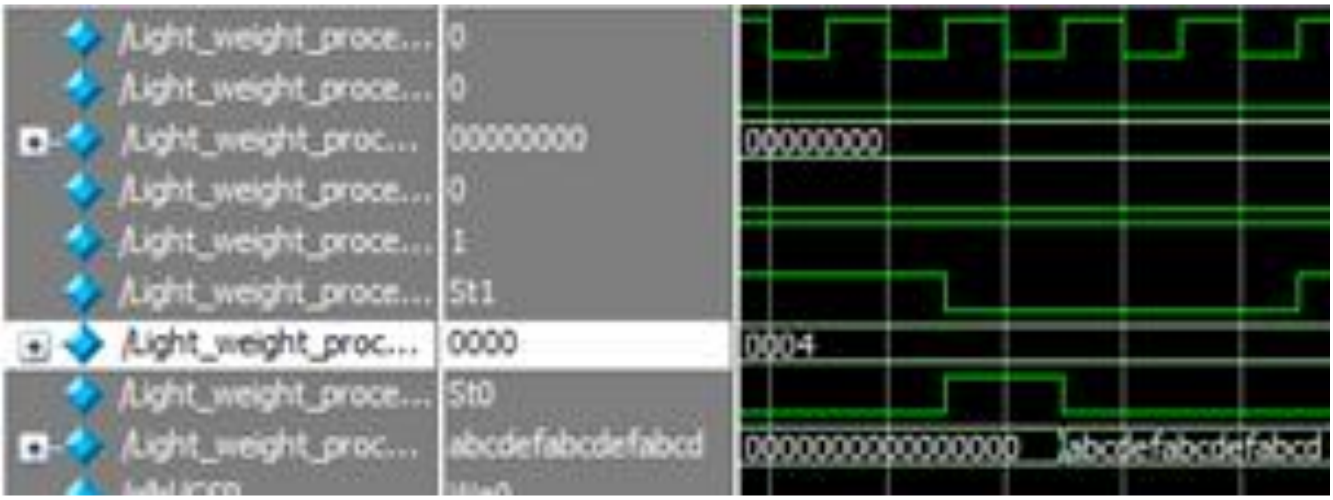
/Light_weight_proce... 0
/Light_weight_proce... 0
/Light_weight_proc... 00000000
/Light_weight_proce... 0
/Light_weight_proce... 1
/Light_weight_proce... St1
/Light_weight_proc... 0000
/Light_weight_proce... St0
/Light_weight_proc... abcdefabcdefabcd
00000000
0004
0000000000000000
abcdefabcdefabcd

Figure 9: Simulation of DES decryption on Multi-processing processor

5. Result Analysis

The implementation of DES algorithm on Multi-processing processor using Verilog code is done. The Synthesis and simulation results are analyzed by dumping the bit-file on the FPGA kit.

The Multi-processing processor simulated output is shown in Figure 5. The simulation result contains the inputs as address and output is the some operation computed on the input data.

The DES encryption for an input data “abcdefabcdefabcd” with key input “1234567812345678” is simulated the encrypted output data is “07a57f8740b619f6”. The simulation is shown in Figure 6.

The DES decryption for an input data “07a57f8740b619f6” with key input “1234567812345678” is simulated the decrypted output data is “abcdefabcdefabcd” which is same as plain text. The simulation is shown in Figure 7.

The DES encryption on Multi-processing processor for an input data “abcdefabcdefabcd” with key input “1234567812345678” is simulated the encrypted output data is “07a57f8740b619f6”. The simulation is shown in Figure 8.

The DES decryption on Multi-processing processor for an input data “07a57f8740b619f6” with key input “1234567812345678” is simulated the decrypted output data is “abcdefabcdefabcd” which is same as plain text. The simulation is shown in Figure 9.

6. Conclusion

The implementation of Multi-processing processor and simulated results are shown. The DES algorithm for encryption and decryption on block of data size 64-bits is simulated and synthesized. The same DES is implemented on Multi-processing processor and the simulation outputs are verified by dumping on FPGA

REFERENCES

[1] Harshali D. “Design and Implementation of Algorithm for DES Cryptanalysis”, 2012.

[2] O P Verma “Performance Analysis of Data Encryption Algorithms”, 2011.

[3] Saeid Taherkhani, Enver Ever, Orhan Gemikonakli “Implementation of Non-Pipelined and Pipelined Data Encryption Standard (DES) Using Xilinx Virtex-6 FPGA Technology”, 2010.

[4] Vikram Pasham and Steve Trimberger “High-Speed DES and Triple DES Encrypt/Decrypt”,2001.

[5] NIST.gov - Computer Security Division - Computer Security Resource Center.

[6] “Data encryption standard (DES)”, National Bureau of Standards (U.S.), Federal Information Processing Standards Publication 46, National Technical Information Service, Springfield, VA,Apr. 1977.

[7] Professor Jaeger Introduction Computer and Network Security “Lecture 5 – Cryptography” CSE497b - Spring 2007 www.cse.psu.edu/~tjaeger/cse497b-s07/

[8] Symmetric-key algorithm - Wikipedia, the free encyclopedia.html

[9] T. Akishita and H. Hiwatari, “Compact Hardware Implementations of the 128-bit Blockcipher CLEFIA.” – SCIS 2011.

[10] A. Poschmann, “Lightweight Cryptography – Cryptographic Engineering for a Pervasive World.” 2009.