DEVELOPMENT OF DES ON FPGA USING VARIABLE TIME DATA PERMUTATION

P. Bharath 1*, K. Naga Lakshmi 2*

1. II. M.Tech (VLSI), Dept of ECE, AM Reddy Memorial College of Engineering & Technology, Petlurivaripalem.

ABSTRACT

This paper presents a data encryption standard algorithm for high performance reconfigurable data security applications. A novel skew core key by combining pipelining concept method is compared to various encryption algorithms. Design of DES is implemented on Xilinx Spartan-3e FPGA technology. In this paper final design and implementation of 16-stage pipelined is achieved efficient encryption rate and number of configurable blocks are used. The proposed method result is very fastest hardware implementation and better area utilization.

Keywords: DES, FPGA, Key scheduling.

I. INTRODUCTION

The modern communication of data security and error correction area most important in the bandwidth limited channels are considered to demand high security. One of the traditional schemes is data compression in that both encrypted and when it is encoded in the transmission, and porn to generate transmission bit error rate also poses a security risk in encrypted is susceptible to statistical analysis based on decryption mechanism. Due to these problems or drawbacks to compare the existing system methods are not reliable and the encrypted data is transferred without compression to utilize the channels very poor performance.

A novel communication method, it can provide quality of secure information without loss data to utilizing channel capability of detecting and correcting errors proposed inn this paper. Here for the encryption and compression scheme use DES algorithm achieve quality of security while it making for compression using Run Length Encoding. When we compress the data the transmission rate will increase and channel utilization efficient performance will get, without loss of information. We have different types of compression techniques have RLE, Hamming code; these methods can
efficiently detect and correct the errors in this application. The receiver side it receives data corrupted from transmitted world which can corrected by the error correction. The proposed methods can be used in all limited bandwidth channels which can demand high security.

II. DESCRIPTION OF DES ALGORITHM

DES is a block of cipher operating on 64-bits block plaintext utilizing a 64-bit key. Fig. 1 shows the algorithm flow of DES, in that every eight bit of 64 bits key is used for parity checking.

The proposed DES algorithm it consists of 16 rounds as shown in Fig. 1. The data is 64-bit firstly it permutated and then divided into 32 bits right (R) and left (L). To processed through DES function as shown in Fig. 2, the right 32 bits are expanded to 48 bits to be processed through XOR function with the round key. The XOR output is converted from 48 bits to 32 bits through substitution boxes (S boxes). The S boxes output is XORed with the 32 bits left and the output is the right to the next round.

The right most bits of the previous of the left round is then next round as illustrated by the following formula:

\[ L_i = R_{i-1}, R_i = L_{i-1} \oplus F(R_{i-1}, K) \quad (1) \]

It consists of 16 rounds key generated from the main key point. The generated
each round has it sub generated key point from the main key point. Fig.4. shows the sequence of generating 16 sub keys. The main key point is permutated according to round number. These round numbers indicates the shift bits, and then the output is permutated by the second permutation.

![Diagram of key generation]

III. PROPOSED METHOD

3.1. Data compression

Compressing data or bit-rate reduction involves entire encoding information using fewer bits than the original representation there is no loss of information. The compression techniques have two types either it can lossy or lossless. The lossless compression reduces the number of redundancy bits and identifying and eliminating statistical redundancy. In this lossless compression there is no loss of information. This process is reducing the size of the data file. The compression technique is useful because it helps to reduce the usage of storage space or transmission capacity.

3.2. Design Pipelining DES algorithm:

Pipelining is wildly use method in large design for speed enhancement. The iterative nature of the DES algorithm makes it ideally suited to pipelining and that can be 4, 6, 8 or 16 stages. The DES algorithm implementation presented in this paper is based on the ECB mode with 16 stages pipelining. Although the ECB mode is less secure than other modes of operation, it is commonly used and its operation can be pipelined as shown in Fig.4.

![Diagram of pipelining DES algorithm]
Implementation of the DES algorithm key schedule employed the same as stated above. The sub-keys are pre-computed that can also be done by direct mapping of given key in required sub-keys but both ways using only wiring resources, so this part will be executed very fast and no optimizations would have any stage pipelined DES design and key-scheduling it is necessary to control the time at which the sub-keys are effective. This is accomplished by the addition of a skew that delays the individual sub-keys by the required amount.

IV. SUMMARY OF PROPOSED IMPLEMENTATION

Implementation of DES algorithm was accomplished on a Spartan 3e device XC3S500e4bg320 using Xilinx foundation, of model-sim 6.3f as a simulation tools are used. The proposed design was used VHDL language. Therefore the schematic design flow of the proposed system is shown in fig. 5.
Fig.5. New DES schematic generated by Xilinx ISE tool.

Fig.5. The simulation window of the new DES.

V. CONCLUSION

The proposed work is an efficient compact implementation of FPGA for pipelined DES based on variable time data permutation is presented. The data is hidden cipher text format that is not understandable and it is variable with time. The proposed security algorithm can be increased 16 stage pipelined design and data block is completely loaded in clock cycles the after the time delay of 16 clock cycle ciphered data will appear on clock cycles. At a clock frequency of 111.882 MHz, the 16-stage pipelined design can encrypt or decrypt data blocks at a rate of 7.16 Gbit/sec and should prove very useful in applications where speed is vital as with real-time communications such as satellite communications and electronic financial transactions etc.

REFERENCES


