ICIC Express Letters
Part B: Applications
Volume **10**, Number **7**, July **2019**

ICIC International ©2019 ISSN 2185-2766
pp. 565–570

IMPLEMENTATION OPTIMIZATION OF THE DES ALGORITHM ON FPGA TO SUPPORT SMARTCARD PROCESSORS

Veronica Ernita Kristianti[1], Eri Prasetyo Wibowo[2,*], Atit Pertiwi[3]
Busono Soerowirdjo[1] and Hamzah Afandi[1]

[1]Faculty of Electrical Engineering
[2]Faculty of Information Technology
[3]Faculty of Information System Technology
Gunadarma University
Jl. Margonda Raya 100, Depok - 16424, West Java, Indonesia
{ veronica; busono; hamzah; atit }@staff.gunadarma.ac.id
*Corresponding author: eri@staff.gunadarma.ac.id

Received November 2018; accepted January 2019

Abstract. *Smartcards that have functions as data storage media and consist of memory and processor, require a security system. The security system on the smartcard is located on a processor called crypto-processor. The security system applied in the smartcard crypto-processor is called cryptographic algorithm. DES (Data Encryption Standard) is a cryptographic algorithm used in smartcard crypto-processors. This research developed the DES algorithm by applying the methods of 8 rounds and 2 cipher functions so that the encryption process time is more optimal. The data encryption process is carried out in parallel by using this method, the initial permutation results from the input data are grouped into 2, right and left, then processed with each cipher function, so that with 8 second rounds the data block has been processed. DES algorithm optimization design is implemented in the VHDL programming language on XC3S1200E Field-Programmable Gate Array (FPGA) devices. The test results show the speed of the encryption process is 9 clocks without latency. The use of resources resulting from the application of the method in this research were 1% slices of Flip-Flop and Latch, 2% slices of LUTs, 71% slices of bonded IOBs and 12% of GCLKs.*
Keywords: Smartcard, Encryption, DES algorithm, FPGA

1. **Introduction.** There are various forms of data and information nowadays, which are text, images, videos, transactions, and others. In this era, most of these data available in digital format are integrated in the form of hardware and stored in a container called a smartcard. Smartcards are plastic cards of the same size as credit cards, and are called smartcards because they contain silicon chips called microcontrollers. The chip consists of memory and processor. To maintain the security and privacy of information and data, cryptographic techniques added to security systems on embedded microprocessor chips [3, 9]. The importance of a security system on the processor is related to data and information stored in it. Cryptographic algorithms that are applied to a processor chip are called crypto-processors. The crypto-processor architecture is shown in Figure 1.

This research focuses on crypto-processor on smartcards which developed the DES (Data Encryption Standard) cryptographic algorithm. The DES algorithm applied to the crypto-processor in this research is the development of Lim's method [11] and the Kaps and Paar's method [4], where DES in Lim's method is applied with 8 cycles and 1 cipher function, while the Kaps and Paar's method applies 8 cycles and 2 cipher functions. Both of these methods avoid using 2 times the Substitution-Box (S-Box) during the process of randomizing data to the cipher function. Based on these researches, to increase the data

DOI: 10.24507/icicelb.10.07.565

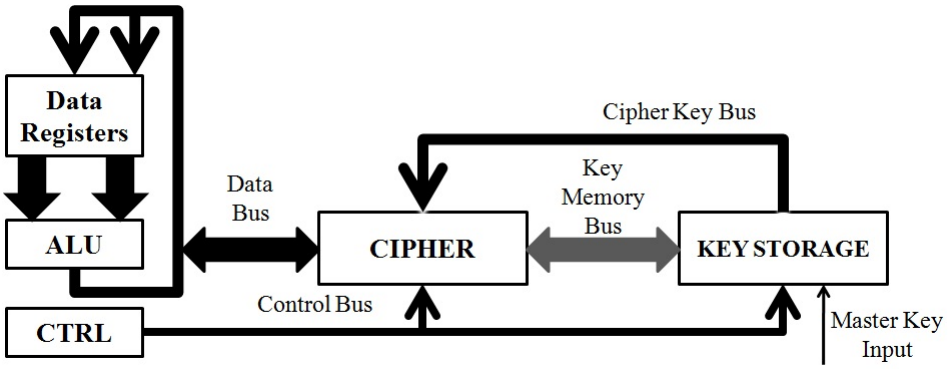

FIGURE 1. Crypto-processor architecture [6]

randomization process with DES algorithm, this research combines the two methods into DES 8 rounds and 2 cipher functions applied to FPGA XC3S1200E.

This paper is organized as follows. The DES algorithm standard is described in Section 2. DES with the methods of 8 rounds and 2 cipher functions are shown in Section 3. The results and analysis of DES 8 rounds and 2 cipher functions into the FPGA XC3S1200E are shown in Section 4. Finally, the conclusions from this research are shown in Section 5.

2. **DES Algorithm Standard.** DES algorithm is recurring symmetric cipher block, operating with permutation, XOR, and substitutions. The algorithm is sequential in every operation and iteration in 16 rounds [5]. The structure of DES algorithm is formed based on principles on the Feistel cipher structure [2, 5]. All operations that iterate in 16 rounds are part of the mode in the DES algorithm [8]. The DES algorithm scheme is shown in Figure 2.

The plain-text 64 bits are rearranged using initial permutations and are called permutation block. The permutation block is then divided into two parts, right and left, L_i and R_i, 32 bits each. The two groups of data are then processed in 16 rounds using cipher function. Cipher function consists of expansion data, XOR with sub-keys, substitution of data with S-Box (Substitution-Box), permutation of P, XOR back with initial data. Two groups of data are then combined and rearranged with final permutation called inverse initial permutation, and the result is called cipher-text as output [7]. The cipher function scheme is shown in Figure 3.

3. **DES 8 Rounds and 2 Cipher Functions.** Optimization of DES algorithm with 8-round method and 2 cipher functions implemented in IC-FPGA was conducted in this research. Optimization is done in both data blocks, right and left, encrypted simultaneously so that the number of radars in the DES algorithm can be optimized and the attention in the algorithm is reduced. The DES algorithm design in this research is shown in Figure 4.

Figure 4 shows that the 8 round DES algorithm consists of 3 main blocks, namely block input, process, and output. The input block is the first process passed by plain text where there is transposition of data units into the Initial Permutation (IP) table. The results of this first transposition is two groups of data L0-32 bits and R0-32 bits. The process block is the center of the encryption process or called the cipher function. The cipher function consists of eXclusive OR (XOR) mathematical operations, permutations and substitutions. L0 and R0 are processed in each cipher function, so that these two data can be processed simultaneously because they are not interdependent or waiting for the process queue. L0 and R0 data are expanded to have the same data width as the sub-key so that it can be processed with XOR operations. XOR results between L0, R0

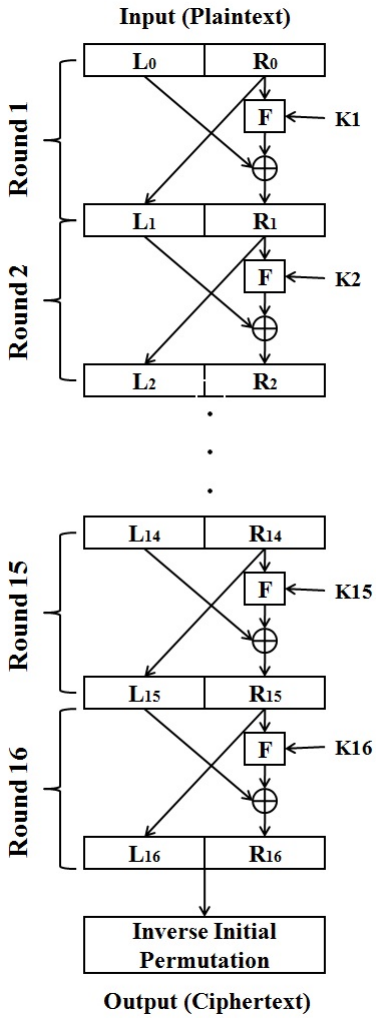

FIGURE 2. DES algorithm scheme [10]

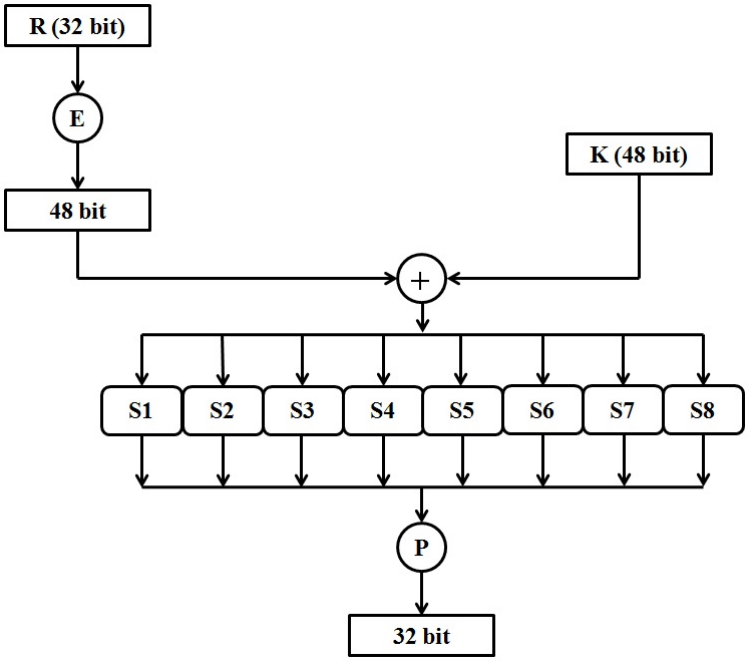

FIGURE 3. Cipher function scheme [1]

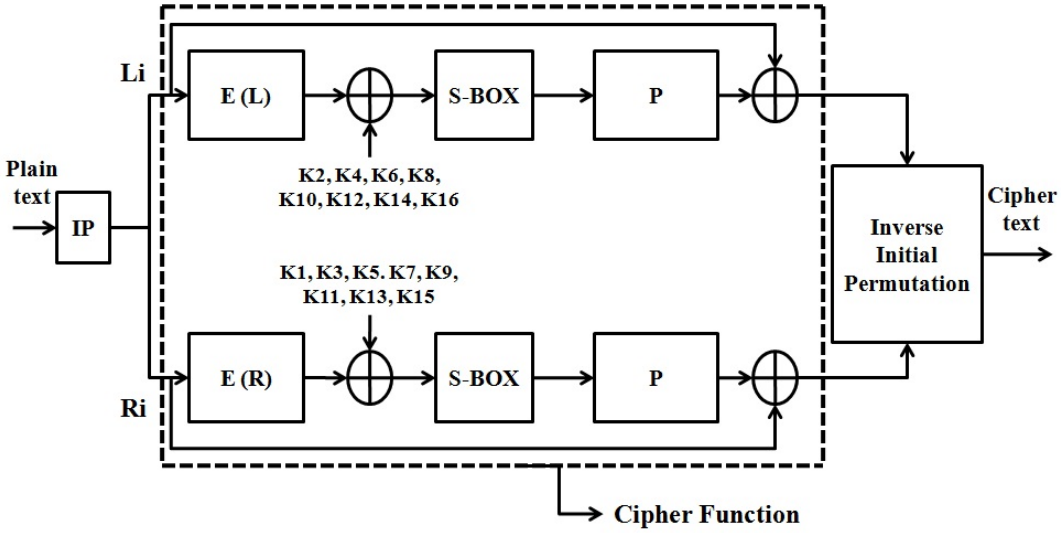

FIGURE 4. Block diagram of architecture 8 round DES algorithm design

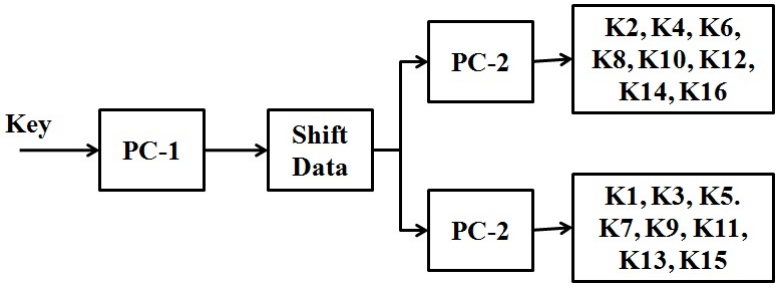

FIGURE 5. Block diagram of sub-key design

and sub-keys are then substituted by using S-Box (Substitution-Box), first cycle using S1, second cycle S2, and so on until the eighth cycle using S8. The use of this method also makes the use of S-Box more efficient because in the DES 16 cycle algorithm, after the 8th cycle, the S-Box usage is repeated. The results of substitution are then permutated with a permutation table known as P permutation. The permutation results are then XOR returned with the initial data unit, in the first cycle at XOR with L0 and R0. This process is repeated until the 8th cycle or until it produces L8 and R8, the two groups of data units are then combined in the final permutation process or known as inverse initial permutation. The data unit has been processed in the final permutation, meaning that the encryption process has been completed and obtained encryption results called cipher-text.

Block diagram of Figure 5 describes the process of sub-key formation, the input key is an external key that can only be known by the owner or user and must be kept confidential so that it is not misused by irresponsible parties. In the process of forming a sub-key, mathematical operation used is permutation namely compression permutation 1 and 2 or PC-1 and PC-2. The width of the data on the formation of sub-keys will decrease, in the permutation of compression 1 number of bits decreases by 8 bits used as parity, so the data width that is processed is 56 bits. Result of PC-1 is then processed by shift operations rotating the data units one, two, three, or four to the left position according to the rotation. After the results of the shift operation, the second permutation is carried out using the table of compression permutation 2 (PC-2). In the second permutation operation the number of bits is reduced by 8 bits, and the result of the PC-2 operation is a sub-key of 16 sub-keys.

DES algorithm method used in this research is 8 round method using 2 cipher functions. These two cipher functions are used to process each data block right and left, so that the process can be run in parallel. This method does not use memory registers but uses Latch to hold data output before the encryption process.

4. **Result and Analysis.** The application of DES algorithm design with 8 round method and 2 cipher functions is performed with FPGA XC3S1200E. The design test results are shown in Figure 6.

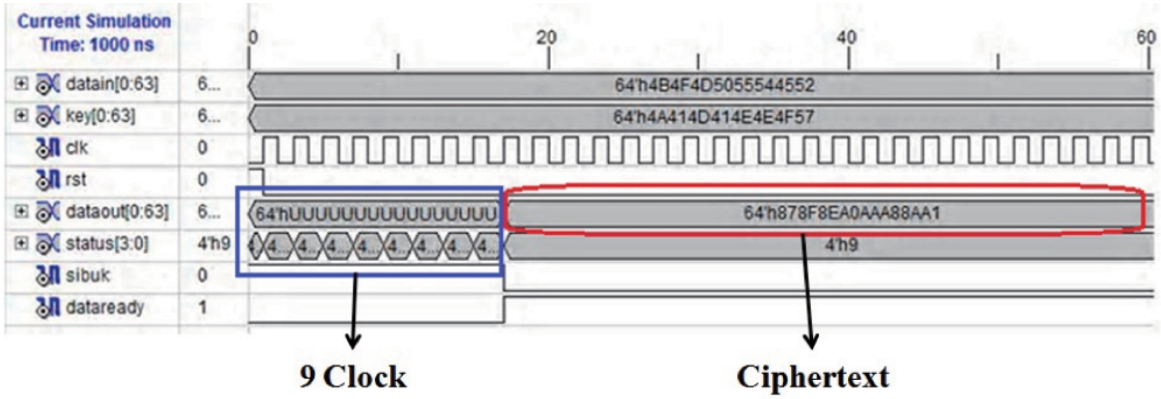

FIGURE 6. Results of 8-cycle DES algorithm design testing

Input data (plain-text) and keys have 64-bit data width. datain [0:63] is the input for plain text that will be encrypted. key [0:63] is input to form sub-key. The results of encryption are shown by dataout [0:63], which means the data with [0:63] is data with a 64-bit capacity. The encryption process in this design is affected by 'first', 'busy', and 'dataready' signals, when 'first' and 'busy' signals are active (high), 64-bit data keys are sent serially via key pins [0:63] and start forming sub-keys. In addition to input data keys, 64-bit plain text data sent serially through data pins [0:63] begins to be processed along with sub-keys to produce text-ciphers. The process of forming sub-keys and the first data randomization process (data initialization) is done in 1 clock. The process of randomizing data to form cipher-text in 8 rounds requires 8 clock processes.

Simulation only requires 9 clocks without latency. The FPGA clock used is 500 MHz with a total period of 2 ns. The test results also provide a summary of device utilization from the DES algorithm design.

Figure 7 shows the summary results of the resource usage required from the DES 8 round algorithm design using XC3S1200E. The result is that it requires 98 slices Flip Flop and Latches or 1% of the 17344 slices provided, LUTs (Look Up Table) of 395 slices or 2% of the 17344 slices provided, bonded IOBs of 136 slices or 71% of the 190 slices provided, and 3 slices Global Clocks (GCLKs) or 12% of the 24 slices provided.

The process of encryption with the 8-round method and 2 cipher functions does not have latency and requires an encryption process of 9 clocks, so that the encryption process time is more optimal than the method used in [4] (16 clock encryption process with latency) and the method performed on [11] (8 clock encryption process with latency), and this makes the encryption process with the 8 round method and 2 cipher functions work more optimally.

5. **Conclusions.** DES design optimization algorithm with 8-round method and 2 cipher functions is applied in XC3S1200E FPGA technology. Both cipher functions are used to process two data blocks, right and left, so that two blocks of data can be encrypted in parallel in 1 time. The design of this method does not use memory registers but uses Latch as a data buffer. The process of randomizing text into a cipher-text is done in 9

DES8NEWFIX_01 Project Status			
Project File:	DES8NEWFIX_01.ise	Current State:	Placed and Routed
Module Name:	DES_TOP	• Errors:	
Target Device:	xc3s1200e-4ft256	• Warnings:	
Product Version:	ISE 9.2i	• Updated:	Mon Oct 22 21:58:19 2018

DES8NEWFIX_01 Partition Summary
No partition information was found.

Device Utilization Summary				
Logic Utilization	Used	Available	Utilization	Note(s)
Total Number Slice Registers	98	17,344	1%	
Number used as Flip Flops	4			
Number used as Latches	94			
Number of 4 input LUTs	395	17,344	2%	
Logic Distribution				
Number of occupied Slices	216	8,672	2%	
Number of Slices containing only related logic	216	216	100%	
Number of Slices containing unrelated logic	0	216	0%	
Total Number of 4 input LUTs	395	17,344	2%	
Number of bonded IOBs	136	190	71%	
IOB Latches	64			
Number of GCLKs	3	24	12%	
Total equivalent gate count for design	3,585			
Additional JTAG gate count for IOBs	6,528			

FIGURE 7. Summary of results of application of 8-round DES algorithm

clocks without latency, with a total period of 2 ns and using frequencies reaching 500 MHz. Based on the results of testing and comparisons with previous research, the encryption process with DES 8 round design and 2 cipher functions can be optimized. Furthermore, implementation of DES 8 rounds and 2 cipher functions into chip form is as future work.

REFERENCES

[1] A. AlAzad, Efficient VLSI implementation of DES and triple DES algorithm with cipher block chaining concept using Verilog and FPGA, *International Journal of Computer Applications*, vol.44, no.16, pp.6-15, 2012.

[2] A. Eshack and S. Krishnakumar, Pipelining concept for low power DES implementation, *International Journal of Computer Applications Technology and Research*, vol.5, no.10, pp.654-656, 2016.

[3] F. Hani, M. Ali, R. Mahmod, M. Rushdan and I. Abdullah, A faster version of Rijndael cryptographic algorithm using cyclic shift and bit wise operations, *International Journal of Cryptology Research*, vol.1, no.2, pp.215-223, 2009.

[4] J.-P. Kaps and C. Paar, Fast DES implementations for FPGAs and its application to a universal key-search machine, *Selected Areas in Cryptography*, pp.234-247, 1998.

[5] J. G. Pandey, A. Gurawa, H. Nehra and A. Karmakar, An efficient VLSI architecture for data encryption standard and its FPGA implementation, *International Conference on VLSI Systems, Architectures, Technology and Applications (VLSI-SATA)*, 2016.

[6] L. Gaspar, *Crypto-Processor – Architecture, Programming and Evaluation of the Security*, Université Jean Monnet – Saint-Etienne, 2012.

[7] M. Noura, H. N. Noura, A. Chehab, M. M. Mansour and R. Couturier, S-DES: An efficient & secure DES variant, *Middle East and North Africa Communications Conference (MENACOMM)*, 2018.

[8] R. Pich, S. Chivapreecha and J. Prabnasak, A single, triple chaotic cryptography using chaos in digital filter and its own comparison to DES and triple DES, *International Workshop on Advanced Image Technology (IWAIT)*, 2018.

[9] S. S. Rani, Triveni. B and S. Umamaheshwar, Implementation of fast pipelined data encryption algorithm (DES) architecture with scan based side channel attack, *International Journal of Electronics Communication and Computer Engineering*, vol.3, no.6, pp.1580-1585, 2012.

[10] W. Stalling, *Cryptography and Network Security Principles and Practice*, 5th Edition, Prentice Hall, 2011.

[11] Y. W. Lim, Efficient 8-cycle DES implementation, *Proc. of the 2nd IEEE Asia Pacific Conference on ASICs*, 2000.