ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 9, December 2013

# Comparative Analysis of DES and S-DES Encryption Algorithm Using Verilog Coding

**Indra Raj Sharma[1], Vipin Gupta[2]**

PG scholar, Electronics & Communication Engineering Department, S.G.V University Jaipur, Rajasthan, India[1]

Assistant Professor, Electronics & Communication Engineering Department, S.G.V University Jaipur, Rajasthan, India[2]

**Abstract:** This paper we present a comparative analysis of Data Encryption Standard and Simplified Data Encryption Standard Algorithm and compare the result of DES and SDES encryption for improve the algorithm performance. The Xilinx Tool is used to synthesize DES and simplified DES algorithm. The performance in terms of delay, power and area of DES and Simplified DES analysed using Cadence Encounter RTL Compiler. The design analysis of Simplified DES shows leakage power is 568nW and Transition power is 169186.883nW, so the total power is 169755.035nW, the delay is 3422ps and die area 1468µm2 on 130nm Process Technology. The design expands the encryption key length, can resist linear cryptanalysis and ensure that there is not "trapdoor" in the password system.

**Keywords**: DES, S-DES, Xilinx, Cadence.

## I. INTRODUCTION

The selective application of technological and related procedural safeguards is an important responsibility of every Federal organization in providing adequate security to its electronic data systems. This publication specifies two cryptographic algorithms, the Data Encryption Standard (DES) and Specified Data Encryption Algorithm (SDEA) which may be used by Federal organizations to protect sensitive data. Protection of data during transmission or while in storage may be necessary to maintain the confidentiality and integrity of the information represented by the data. The algorithms uniquely define the mathematical steps required to transform data into a cryptographic cipher and also to transform the cipher back to the original form. The Data Encryption Standard is being made available for use by Federal agencies within the context of a total security program consisting of physical security procedures, good information management practices, and computer system/network access controls DES (Data Encryption Standard) can be regarded as a technology of data encryption standard which is widely used in the field of data encryption with good safety performance.

Implementation of DES is usually divided into software and hardware approaches. The software solution is generally slow with encryption speed less than 150 Mb/s. The software method also has security problems, while the hardware encryption can be a better choice. FPGA (field programmable gate array) implementation of DES encryption algorithm performs at much faster data-rates and provides better security than equivalent software implantations.

This paper focuses discussion on an improved method of S-DES over DES Algorithm. It has higher speed in hardware for implementation.

## II. BASIC PRINCIPLE OF DES ALGORITHM

In DES algorithm, it uses of a variety of cryptographic techniques synthetically, such as the permutation, the replacement, algebra. The alternation of substitution from the S-boxes, and permutation of bits from the S-box and E-expansion provides so-called "confusion and diffusion", respectively, a concept is identified by Claude Shannon in the 1940s as a necessary condition for a secure yet practical cipher.

DES is the archetypal block cipher — an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another ciphertext bits string of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize

Indra Raj Sharma[1] PG scholar is with the Electronics & Communication Engineering Department, S.G.V University Jaipur, Rajasthan, India ( phone: 09829704941 ; e-mail – indrarajsharma7@gmail.com).
Vipin Gupta[2] Assistant Professor is with the Electronics & Communication Engineering Department, S.G.V University Jaipur, Rajasthan, India.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 9, December 2013

be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits, however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits, and it is usually quoted as such There is an initial and final permutation, termed IP and FP, which are inverses (IP "undoes" the action of FP, and vice versa). The algorithm's overall structure has 16 identical stages of processing, termed rounds. Before the main rounds, the block is divided into two 32-bit halves and processed alternately; the 32-bit half-block is expanded to 48 bits using the expansion permutation, denoted E in the diagram, by duplicating some of the bits. This criss-crossing is known as the Feistel scheme. The Feistel structure ensures that decryption and encryption are very similar processes. The rest of the algorithm is identical. This greatly simplifies implementation, particularly in hardware, as there is no need for separate encryption and decryption algorithms.

The algorithm generates the subkeys. Initially, 56 bits of key are selected from the initial 64 by Permuted Choice 1, The 56 bits are then divided into two 28-bit halves, each half is thereafter treated separately. In successive rounds, both halves are rotated left by one or two bits (specified for each round), then 48 subkey bits are selected by Permuted Choice2, after mixing in the subkey, the block is divided into eight 6-bit pieces before processing by the S-boxes, or substitution boxes. Each of the eight S-boxes replaces its six input bits with four output bits according to a non-linear transformation, provided in the form of a lookup table. The S-boxes provide the core of the security of DES — without them, the cipher would be linear, and trivially breakable. The rotations mean that a different set of bits is used in each subkey. The 16 operations DES are achieved by repeating the operation 16 times.

## III. BASIC FRAMEWORK OF DES ALGORITHM

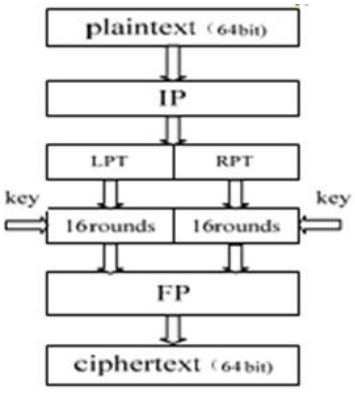


Figure 1. Overall structure of DES algorithm

The advantage of DES encryption and decryption is the high speed and easy realization of algorithms. Generally speaking it is very successful, but there have some weaknesses and shortcomings inevitably: short key length side, there are four so-called weak keys and six pairs of semi-weak keys. Encryption with one of the pair of semi-weak keys, the existence of complementary symmetry, S-box criteria for the design of the box does not open, and may contains "trapdoor", lower the number of DES rounds of anti-poor linear cryptanalysis.

## IV. IMPROVED S-DES ALGORITHM

Simplified DES is an encryption algorithm used for educational purposed rather than a secure encryption algorithm. It has similar properties and structure to DES (secure encryption algorithm) with much smaller parameters. The simplified DES algorithm takes an 8-bit block of plain text and a 10-bit key as input and produces an 8-bit block of Cipher text as output. Simplified DES, developed by the Professor Edward Schaefer of Santa Clara University, is an educational rather than a secure encryption algorithm. It has similar properties and structure to DES with much smaller parameters.

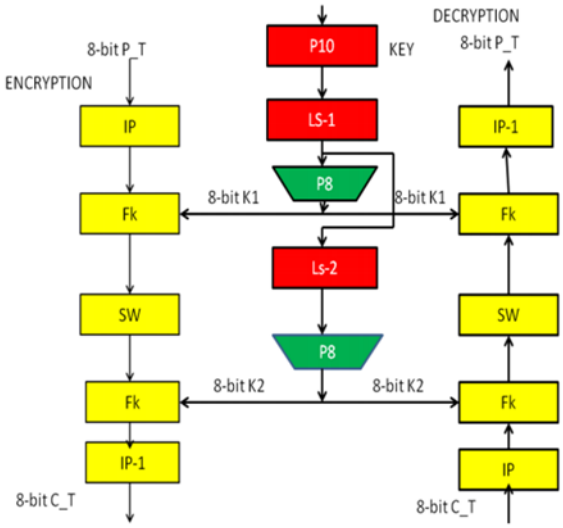


Figure2: Simplified DES scheme

## V. XILINX IMPLEMENTATION

### A. Designing Structures

The realization of the structure of DES is a cascade module to form a pipeline structure. It is an archetypal iterative block cipher algorithm, which based on a lot of combinations, such as repeated permutation, shift, XOR logic operation, and so on, moreover, it is a simple data path. DES algorithm coding process can be pipelined to achieve, it will solve for the depth of the pipeline 16 as the 16 times a cycle of iteration. As the hardware and other reasons, this article takes the simplified design of the DES to illustrate the effect design by an example.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 9, December 2013

System is designed the main input for the system clock signal clk1, 8-bit data input IPy, a 10-bit encryption key input key, two 8-bit of pre-generated sub-keys KEY1, KEY2 directly into the main program. 8-bit output signal is the ciphertext [6]. The design of the structure of the framework is represented in Figure 2.

### B. Simplified key generation

The algorithm generates the subkeys in 16 rounds. For instance key1, this module's input has system clock clk0, 10-bit key input key, the output have 16-eight bits subkeys. According with 16 cascade pipeline modules of iterative operations, the design keeps the 64-bit block size of DES, and could act as a "drop-in" replacement subkey generation module also drops in the pipeline structure of register. S-DES depends on the use of a 10-bit key shared between sender and receiver. From this key, two 8-bit sub keys are produced for uses in particular stage are produced for use in particular stages of the encryption and decryption algorithm.

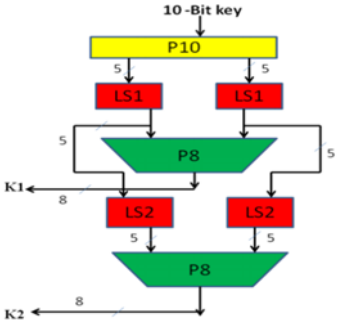


Figure 3 S-DES Key Generation

Figure 3 depicts the stages followed to produce the subkeys. First permute the key in the following fashion. Let the 10-bit key be designated as (k1, k2, k3, k4, k5, k6, k7, k8, k9, k10). Then the permutation P10 is defined as –

P10 (k1, k2, k3, k4, k5, k6, k7, k8, k9, k10) = (k3, k5, k2, k7, k4, k10, k1, k9, k8, k6)

DES algorithm has sixteen rounds identical iterative operation, and every round operation needs a key to assist in the XOR, the subkey has a fixed relation with initial key.

## VI. SYNTHESIS RESULTS

The performance in terms of delay, power and area of DES and Simplified DES analysed using Cadence Encounter RTL Compiler. The design analysis of Simplified DES shows leakage power is 568nW and Transition power is 169186.883nW, so the total power is 169755.035nW, the delay is 3422ps and die area 1468µm2 on 130nm Process Technology.

First we write HDL file (Verilog or VHDL) then we are setting path of standard cell as well as output directory (Result). then we are loading HDL files and perform elaboration then applying constrains then we are optimize our design after that we are synthesize the design and analyse if all constrains are meet than we are done placement and Routing and then generating Netlist so we can able to generate layout for chip fabrication so we are calculating power, delay & area and critical path for delay from above procedure.

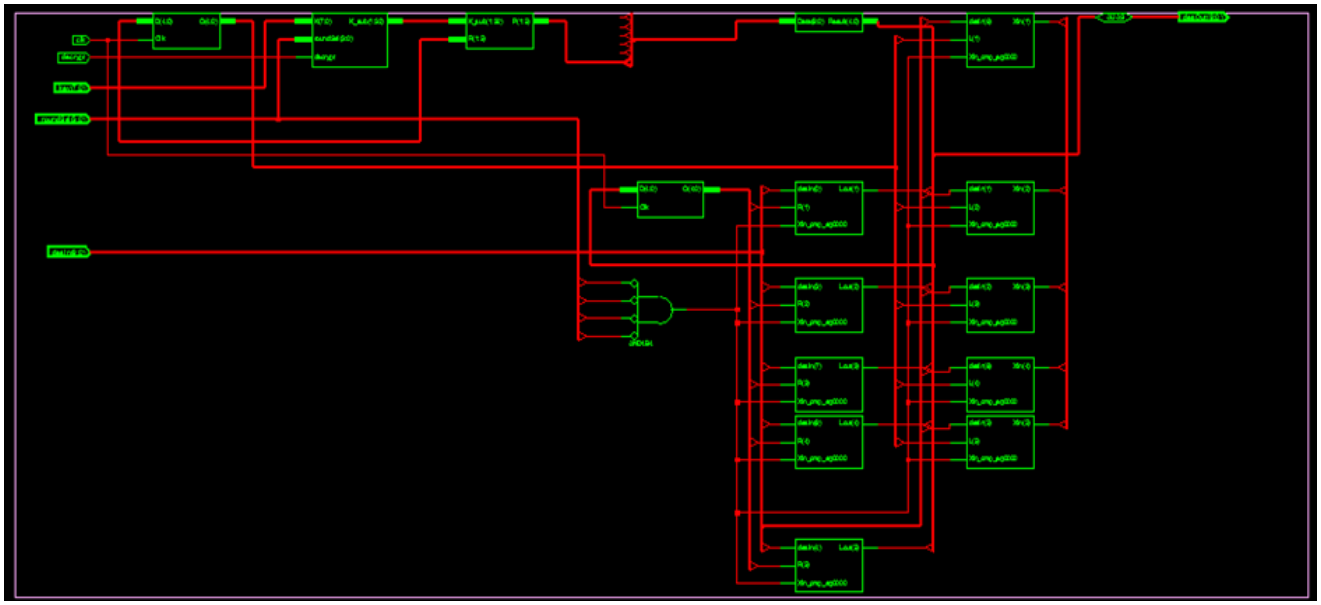

Figure 4 Results Generated using SDES Top Module for hardware

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 9, December 2013

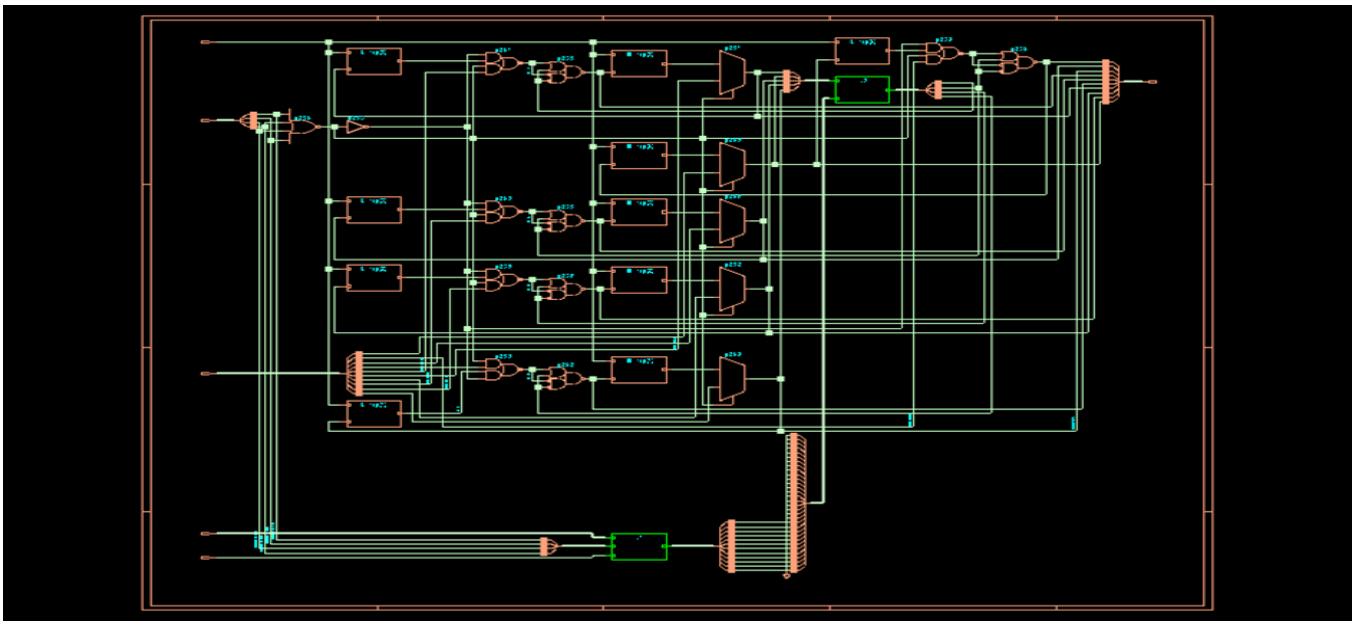

Figure 5 Results Generated using SDES Top Module

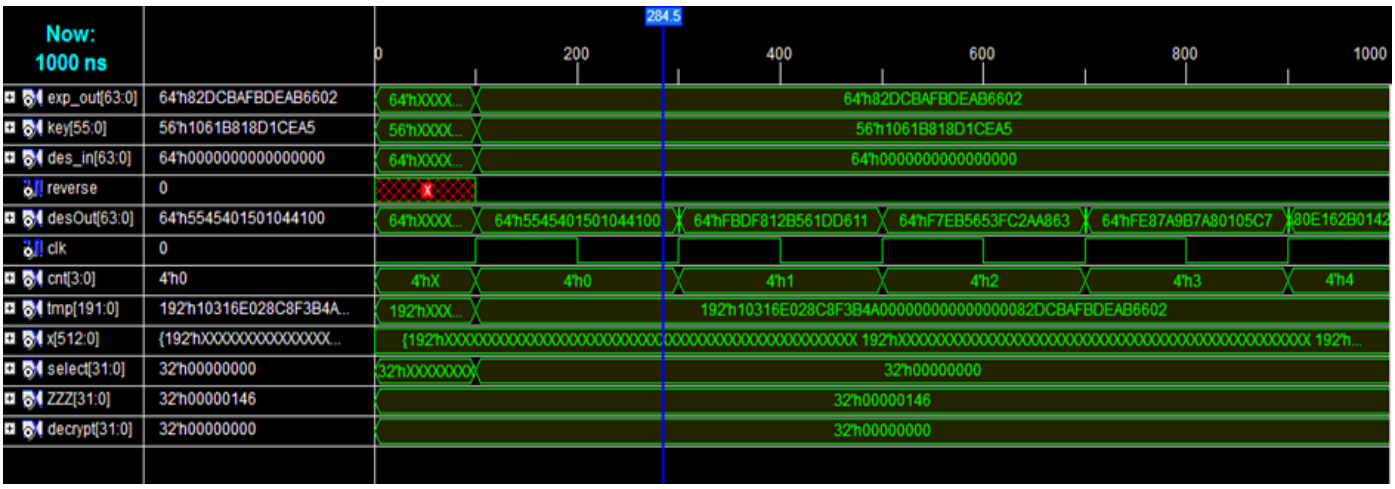


Figure 6 The Critical Path

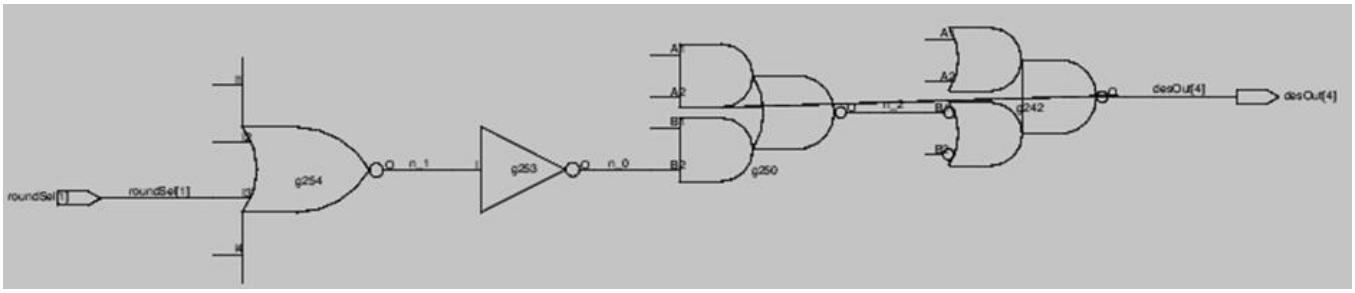


Figure 7 The schematic Diagram

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 9, December 2013

So this algorithm sets up relation scheme between key and subkey, and directly uses this scheme when the hardware implements. When the hardware implement, it can customize every key by selected the left shift digit of the key of mutation and combination, the design of mutation and combination and subkey can preplan generation.

This design makes subkeys into rom after preplan generation, affording date stream to pipeline apartment. The structure is followed in Figure 2. This relation scheme can avoid interference among subkey by preplan generation, and help the subkey dynamic dispensing on pipeline. This way simplify the generation of subkey, making best use the hardware resource effectively.

## VII. SYNTHESIS RESULTS

The performance in terms of delay, power and area of DES and Simplified DES analysed using Cadence Encounter RTL Compiler. The design analysis of Simplified DES shows leakage power is 568nW and Transition power is 169186.883nW, so the total power is 169755.035nW, the delay is 3422ps and die area 1468µm2 on 130nm Process Technology.

First we write HDL file (Verilog or VHDL) then we are setting path of standard cell as well as output directory (Result). then we are loading HDL files and perform elaboration then applying constrains then we are optimize our design after that we are synthesize the design and analyse if all constrains are meet than we are done placement and Routing and then generating Netlist so we can able to generate layout for chip fabrication so we are calculating power, delay & area and critical path for delay from above procedure.

The critical path found in between roundSel(1) and desOut(4). The Slack time of this critical path is 3422 ps. So for faster performance we can increase clock speed and able to fix clock at period of 5ns. We are generate Netlist so we can analyse and able to generate the schematic Diagram and layout The schematic diagram shows the interconnection of logic gates and flip - flops which perform the S-DES algorithm, and this schematic diagram is used to generate Netlist so we can design the simplified form of layout.

## VIII. CONCLUSION

In this paper, the performance in terms of delay, power and area of DES and Simplified DES analysed using Cadence Encounter RTL Compiler. The design analysis of Simplified DES shows leakage power is 568nW and Transition power is 169186.883nW, so the total power is 169755.035nW, the delay is 3422ps and dies area 1468µm2 on 130nm Process Technology. It is more satisfactory options for both algorithm in terms of utilization and the speed of execution.

## REFERENCES

[1] William Stallings "Cryptography and Network Security", Fifth Edition, Prentice Hall 2010, ISBN-10: 0136097049.
[2] Reaffirmed "Federal information processing standards publication", U.s. department of commerce/national institute of standards and technology, 1999 October 25
[3] FU Li, PAN Ming, "A Simplified FPGA Implementation Based on an Improved DES Algorithm", 2009 Third International Conference on Genetic and Evolutionary Computing, 978-0-7695-3899-0/09 © 2009 IEEE
[4] S. Drabowitch, A. Papiernik, H. Griffiths, J. Encinas and B. L. Smith, "Modern Antennas", 1st Edition, Chapman & Hall, 1998.
[5] Nalini N', G RaghavendraRao, "Cryptanalysis of Simplified Data Encryption Standard via Optimization Heuristics", PP 0-7803-9588-3/05 ©2005 IEEE.
[6] Baocang Wang, Qianhong Wu, Yupu Hu: A Knapsack Based Probabilistic Encryption Scheme, On Line March 2007.
[7] Blum L., Blum M , Shub M. : A simple unpredictable pseudo random number generator , SIAM J. compute , 1986, 15, (2), pp 364-383.
[8] Brics: Universally comparable notions of key exchange and secure channels, Lecture Notes in Computer Science, Springer, Berlin, March 2004.
[9] Bruce Scheneier: Applied cryptography (John Wiley & sons (ASIA) Pvt. Ltd.
[10] Carlone Fontaine & Fabien Galand: A Survey of Homomorphic Encryption for non-specialists, EURASIP Journal,Vol 07, Article 10.
[11] Donavan G.Govan, Nathen Lewis: Using Trust for Key Distribution & Route Selection in Wireless Sensor Networks, International Conference on Network Operations & Management, IEEE Symposium 2008, PP 787-790.