VLSI Implementation of Data Encryption Standard Algorithm

Naveen Kumar, B.Venu Gopal

Abstract—There are two main types of cryptography in use today –symmetrico rsecret key cryptography and a symmetric or public key cryptography. Symmetric key cryptography is the oldest type whereas asymmetric cryptography is only being used publicly since the late 1970's 1 . Asymmetric cryptography was a major milestone in the search for a perfect encryption scheme.

Secret key cryptography goes back to at least Egyptian times and is of concern here. It involves the use of only one key which is used for both encryption and decryption

(hence the use of the term symmetric). Figure 2.1 depicts this idea. It is necessary for security purposes that the secret key never be revealed

To accomplish encryption, most secret key algorithms use two main techniques known assubstitutionandpermutation. Substitution is simply a mapping of one value to another whereas permutation is a reordering of the bit positions for each of the inputs. These techniques are used a number of times in iterations called rounds. Generally, the more rounds there are, the more secure the algrithm. A non-linearity is also introduced into the encryption so that decryption will be computationally infeasible 2 without the secret key. This is achieved with the use of S-boxes which are basically non-linear substitution tables where either the output is smaller than the input or viceversa.

Index Terms—cryptography, encrypt ion

I. INTRODUCTION

Up until recently, the main standard for encrypting data was a symmetric algorithm known as theData Encryption Standard (DES). However, this has now been replaced by a new standard known as theAdvanced Encryption Standard (AES)which we will look at later. DES is a 64 bitblock cipherwhich means that it encrypts data 64 bits at a time. This is contrasted to astream cipherin which only one bit at a time (or sometimes small groups of bits such as a byte) is encrypted. DES was the result of a research project set up by International Business Machines (IBM) corporation in the late 1960's which resulted in a cipher known as LUCIFER. In

the early 1970's it was decided to commercialise LUCIFER and a number of significant changes were introduced. IBM was not the only one involved in these changes as they sought technical advice from the National Security Agency (NSA) (other outside consultants were involved but it is likely that the NSA were the major contributors from a technical point of view). The altered version of LUCIFER was put forward as a proposal for the new national encryption standard requested by the National Bureau of Standards (NBS) 3 . It was finally adopted in 1977 as the Data Encryption Standard - DES (FIPS PUB 46). Some of the changes made to LUCIFER have been the subject of much controversy even to the present day. The most notable of these was the key size. LUCIFER used a key size of 128 bits however this was reduced to 56 bits for DES. Even though DES actually accepts a 64 bit key as input, the remaining eight bits are used for parity checking and have no effect on DES's security. Outsiders were convinced that the 56 bit key was an easy target for a brute force attack 4 due to its extremely small size. The need for the parity checking scheme was also questioned without satisfying answers. Another controversial issue was that the S-boxes used were designed under classified conditions and no reasons for their particular design were ever given. This led people to assume that the NSA had introduced a "trapdoor" through which they could decrypt any data encrypted by DES even without knowledge of the key. One startling discovery was that the S-boxes appeared to be secure against an attack known as Differential Crypt analysis which was only publicly discovered by Biham and Shamir in 1990. This suggests that the NSA were aware of this attack in 1977; 13 years earlier! In fact the DES designers claimed that the reason they never made the design specifications for the S-boxes available was that they knew about a number of attacks that weren't public included in Section 4. knowledge at the time and they didn't want them leaking - this is quite a plausible claim as differential cryptanalysis has shown. However, despite all this controversy, in 1994 NIST reaffirmed DES for government use for a further five years for use in areas other than "classified". DES of course isn't the only symmetric cipher. There are many others, each with vary- ing levels of complexity. Such ciphers include: IDEA, RC4, RC5, RC6 and the new Advanced Encryption Standard (AES). AES is an important algorithm and was originally meant to replace DES (and its more secure variant triple DES) as the standard algorithm fornon-classified material. However as of 2003, AES with key sizes of 192 and 256 bits has been found to be secure enough to protect information up to top secret. Since its creation, AES had underdone intense scrutiny as one would expect for an algorithm that is to be used as the standard. To date it has withstood all attacks but the search is still on and it remains to be seen whether or not this will last.

II. CRYPTOGRAPHY TECHNIQUES

There are two techniques used for data encryption and decryption, which are:

2.1 Symmetric Cryptography

If sender and recipient use the same key then it is known as symmetrical or private key cryptography. It is always suitable for long data streams. Such system is difficult to use

Manuscript Received on November, 2012.

Naveen Kumar, M.Tech ECE Department,JNTU Kakinada University/ Kaushik College of Engineering /Visakhapatnam, India.

B.Venu Gopal, Assoc .Professor, Dept. of ECE, Kaushik College of Engineering /visakhapatnam, India.

in practice because the sender and receiver must know the key. It also requires sending the keys over a secure channel from sender to recipient. There are two methods that are used in symmetric key cryptography: block and stream.

The block method divides a large data set into blocks (based on predefined size or the key size), encrypts each block separately and finally combines blocks to produce encrypted data.

The stream method encrypts the data as a stream of bits without separating the data into blocks. The stream of bits from the data is encrypted sequentially using some of the results from the previous bit until all the bits in the data are encrypted as a whole.

2.2 Asymmetric Cryptography

If sender and recipient use different keys then it is known as asymmetrical or public key cryptography. The key used for encryption is called the public key and the key used for decryption is called the private key. Such technique is used for short data streams and also requires more time to encrypt the data. Asymmetric encryption techniques are almost 1000 timess lower than symmetric techniques, because they require more computational processing power. To get the benefits of both methods, a hybrid technique is usually used. In this technique, asymmetric encryption is used to exchange the secret key; symmetric encryption is then used to transfer data between sender and receiver.

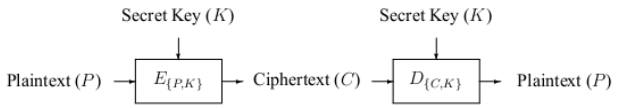

Figure 2.1: Secret key encryption.

III. INNER WORKING OF DES

DES (and most of the other major symmetric ciphers) is based on a cipher known as the Feistel block cipher. This was a block cipher developed by the IBM cryptography researcher Horst Feistel in the early 70's. It consists of a number of rounds where each round contains bit-shuffling, non-linear substitutions (S-boxes) and exclusive O operations. Most symmetric encryption schemes today are based on this structure (known as afeistel network). As with most encryption schemes, DES expects two inputs - the plaintext to be encrypted and the secret key. The manner in which the plaintext is accepted, and the key arrangement used for encryption and decryption, both determine the type of cipher it is. DES is therefore a symmetric, 64 bit block cipheras it uses the same key for both encryption and decryption and only operates on 64 bit blocks of data at a time 5 (be they plaintext or ciphertext). The key size used is 56 bits, however a 64 bit (or eight-byte) key is actually input. The least significant bit of each byte is either used for parity (odd for DES) or set arbitrarily and does not increase the security in any way. All blocks are numbered from left to right which makes the eight bit of each byte the parity bit. Once a plain-text message is received to be encrypted, it is arranged into 64 bit blocks required for input. If the number of bits in the message is not evenly divisible by 64, then the last block will be padded. Multiple permutations and substitutions are incorporated throughout in order to increase the difficulty of performing a cryptanalysis on the cipher. However, it is generally accepted that the initial and final permutations offer little or no contribution to the security of DES and in fact some software implementations omit them (although strictly speaking these are not DES as they do not adhere to the standard).

Overall structure:

Figure 2.2 shows the sequence of events that occur during an encryption operation. DES performs an initial permutation on the entire 64 bit block of data. It is then split into 2, 32 bit sub-blocks, Li andRi which are then passed into what is known as a round(see figure 2.3), of which there are 16 (the subscript i in Li andRi indicates the current round). Each of the rounds are identical and the effects of increasing their number is twofold - the algorithms security is increased and its temporal efficiency decreased. Clearly these are two conflicting outcomes and a compromise must be made. For DES the number chosen was 16, probably to guarantee the elimination of any correlation between the ciphertext and either the plaintext or key 6 . At the end of the 16th round, the 32 bitLi andRi output quantities are swapped to create what is known as thepre-output. This [R16, L 16] concatenation is permuted using a function which is the exact inverse of the initial permutation. The output of this final permutation is the 64 bit ciphertext.

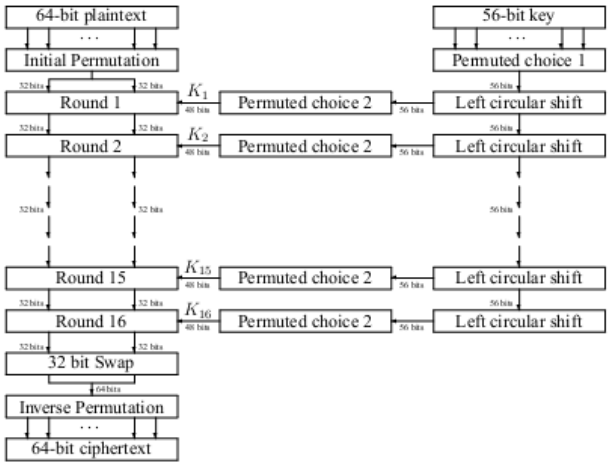

Figure 2.2: Flow Diagram of DES algorithm for encrypting data.

So in total the processing of the plaintext proceeds in three phases as can be seen fromthe left hand side of figure 2.2:

1. Initial permutation (IP - defined in table 2.1) rearranging the bits to form the "permuted input". 2. Followed by 16 iterations of the same function (substitution and permutation).

The output of the last iteration consists of 64 bits which is a function of the plaintext and key. The left and right halves are swapped to produce the preoutput. 3. Finally, the preoutput is passed through a permutation (IP −1 - defined in table 2.1) which is simply the inverse of the initial permutation (IP). The outputofIP−1 is the 64-bit cipher text.

(a) Initial Permutation (IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

(b) Inverse Initial Permutation (IP^{-1})

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

(c) Expansion Permutation (E)

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

(d) Permutation Function (P)

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Table 2.1: Permutation tables used in DES.

As figure 2.2 shows, the inputs to each round consist of the Li, R i pair and a 48 bit sub key which is a shifted and contracted version of the original 56 bit key. The use of the key can be seen in the right hand portion of figure 2.2:

• Initially the key is passed through a permutation function (PC1 - defined in table 2.2)

• For each of the 16 iterations, a subkey (Ki) is produced by a combination of a left circular shift and a permutation (PC2-defined in table 2.2) which is the samefor each iteration. However, the resulting subkey is different for each iteration because of repeated shifts.

(a) Input Key

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

(b) Permuted Choice One (PC-1)

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

(c) Permuted Choice Two (PC-2)

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

(d) Schedule of Left Shifts

Round number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Table 2.2: DES key schedule.

Details of individual rounds:

Details of an individual round can be seen in figure 2.3. The main operations on the data are encompassed into what is referred to as thecipher functionand is labeledF. This function accepts two different length inputs of 32 bits and 48 bits and outputs a single 32 bit number. Both the data and key are operated on in parallel, however the operations are quite different. The 56 bit key is split into two 28 bit halvesCi andDi (C and D being chosen so as not to be confused with L and R). The value of the key used in any round is simply a left cyclic shift and a permuted contraction of that used in the previous round. Mathematically, this can be written

$$C_i = Lcs_i(C_{i-1}), D_i = Lcs_i(D_{i-1})$$

$$K_i = PC_2(C_i, D_i)$$

As where Lcsi is the left cyclic shift for round i,Ci and Di are the outputs after the shifts, P C2 (.) is a function which permutes and compresses a 56 bit number into a 48 bit number and Ki is the actual key used in round i. The number of shifts is either one or two and is determined by the round number i. Fori ={1,2,9,16}the number of shifts is one and for every other round it is two (table 2.2).

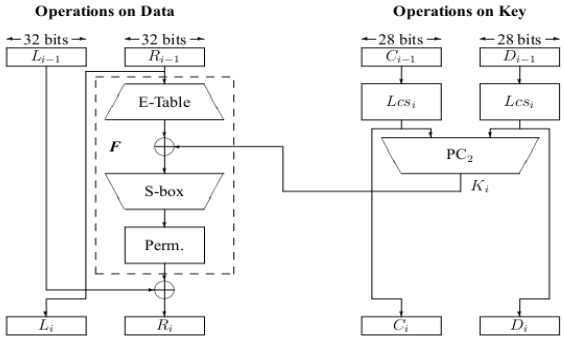

Figure 2.3: Details of a single DES round.

The common formulas used to describe the relationships between the input to one round and its output (or the input to the next round) are:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus \boldsymbol{F}(R_{i-1}, K_i)$$

Where L and R have their usual meaning andF(.) is the cipher function. This function Fis the main part of every round and consists of four separate stages (see figure 2.4): 1. The E-box expansion permutation - here the 32-bit input data fromRi−1is expanded and permuted to give the 48 bits necessary for combination with the 48 bit key (defined in table 2.1). The E-box expansion permutation delivers a larger output by splitting its input into 8, 4-bit blocks and copying every first and fourth bit in each block into the output in a defined manner. The security offered by this operation comes from one bit affecting two substitutions in the S-boxes. This causes the dependency of the output bits on the input bits to spread faster, and is known as the avalanche affect.

2. The bit by bit addition modulo 2 (or exclusive OR) of the E-box output and 48 bit subkeyKi

3. The S-box substitution - this is a highly important substitution which accepts a 48-bit input and outputs a 32-bit number (defined in table 2.3). The S-boxes are the only non-linear operation in DES and are therefore the most important part of its security. They were very carefully designed although the conditions they were designed under has been under intense scrutiny since DES was released. The reason was because IBM had already designed a set of S-boxes which were completely changed by the NSA with no explanation why 7 . The input to the S-boxes is 48 bits long arranged into 8, 6 bit blocks (b 1 , b2, . . . , b6).There are 8 S-boxes (S1, S2, . . . , S8) each of which accepts one of the 6 bitblocks. The output of each S-box is a four bit number. Each of the S-boxes can be thought of as a4×16matrix. Each cell of the matrix is identified by acoordinate pair (i, j), where0≤i ≤3and0≤j ≤15. The value of i is taken as the decimal representation of the first and last bits of the input to each S-box, i.e. Dec(b1b6) = i and the value of j is take from the decimal representation of the inner four bits that remain, i.e. Dec(b2b3b4b5) = j. Each cell within the S-box matrices contains a 4-bit number which is output once that particular cell is selected by the input. 4. The P-box permutation - This

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

simply permutes the output of the S-box without changing the size of the data (defined in table 2.1). It is simply a permutation and nothing else. It has a one to one mapping of its input to its output giving a 32 bit output from a 32 bit input.

IV. OTHER POINTS OF NOTE

Having looked at DES in some detail a brief look at some other points is in order. These include decryption, modes of operation, security etc.

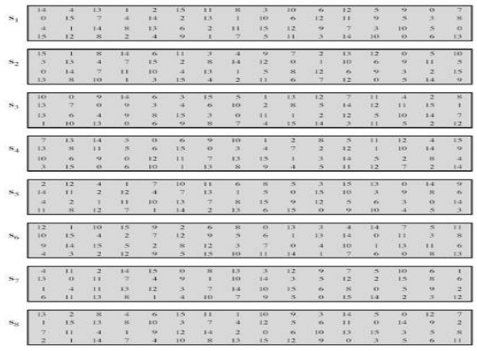

Table 2.3: S-box details.

Modes of operation The DES algorithm is a basic building block for providing data security. To apply DES in a variety of applications, five modes of operation have been defined which cover virtually all variation of use of the algorithm and these are shown in table 2.4.

Figure 2.4: The complex F function of the DES algorithm.

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of 64 plaintext bits is encoded independently using the same key.	•Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext.	•General-purpose block-oriented transmission •Authentication
Cipher Feedback (CFB)	Input is processed J bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	•General-purpose stream-oriented transmission •Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding DES output.	•Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	•General-purpose block-oriented transmission •Useful for high-speed requirements

Table 2.4: DES modes of operation.

DES decryption

The decryption process with DES is essentially the same as the encryption process and is as follows:

• Use the ciphertext as the input to the DES algorithm butuse the keys Ki in reverse order. That is, use K16 on the first iteration,K15 on the second untilK1 which is used on the 16th and last iteration.

Avalanche effect:

A desirable property of any encryption algorithm is that a small change in either plain- text or key should produce significant changes in the ciphertext. DES exhibits a strong avalanche effect. Table 2.5 illustrates this.

(a) Change in Plaintext		(b) Change in Key	
Round	Number of bits that differ	Round	Number of bits that differ
0	1	0	0
1	6	1	2
2	21	2	14
3	35	3	28
4	39	4	32
5	34	5	30
6	32	6	32
7	31	7	35
8	29	8	34
9	42	9	40
10	44	10	38
11	32	11	31
12	30	12	33
13	30	13	28
14	26	14	26
15	29	15	34
16	34	16	35

Avalanche effect - a small change in the plaintext produces a significant change in the ciphertext.

V. CONCERN ABOUT THE ALGORITHM

As mentioned initially, since its adoption as a federal standard there have been concerns

about the level of security provided by DES in two areas, Key size and nature of the algorithm.

• 56 bit key length (approx7.2×10 16) on initial consideration brute-force at- tack seems impractical. However with a massively parallel machine of about 5000 nodes with each node capable of achieving a key search rate of 50 mil-lion keys/sec, the time taken to do a brute-force search is approximately 100 hrs which is far from excessive.

• The nature of DES algorithm: of more concern is that cryptanalysis is possible by exploiting the characteristics of DES. The focus is the eight S-boxes used in each iteration. The design criteria for the complete algorithm has never been

published and there has been speculation that the boxes were constructed in such a way that cryptanalysis is possible by an opponent who knows the weakness in the S-boxes. Although this has not been established, the US government's"clipper project" raises many question. These are the main reasons DES is now being replaced by the AES standard .

VI. IMPLEMENTATION AND RESULTS

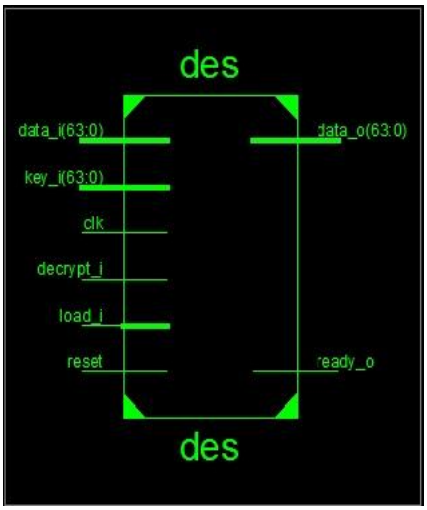

Fig. 2.5: DES top module.

Fig. 2.6: Output waveform for DES Encryption

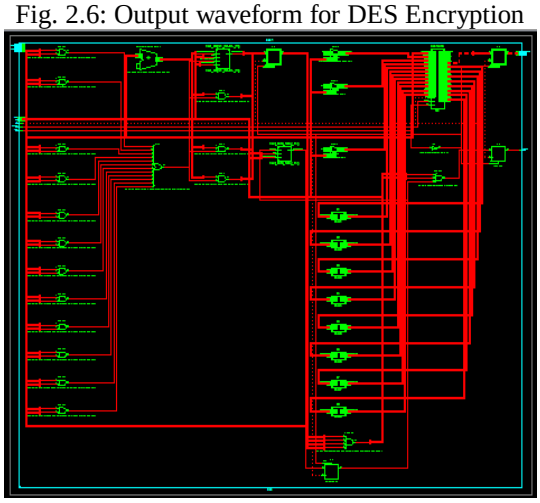

Fig:2.7 RTL Schematic

The DES module was implemented in Xilinx Spartan 3E fpga Xc3s200 and the simulation results were shown in the above figures.

Device Utilization Summary (estimated values)			[-]
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slices	359	1920	18%
Number of Slice Flip Flops	190	3840	4%
Number of 4 input LUTs	698	3840	18%
Number of bonded IOBs	189	173	109%
Number of GCLKs	1	8	12%

REFERENCES

1. National Bureau of Standards – Data Encryption Standard, Fips Publication 46,1977.
2. O.P. Verma, Ritu Agarwal, Dhiraj Dafouti,Shobha Tyagi — Performance Analysis Of Data Encryption Algorithms — , 2011
3. Gurjeevan Singh, Ashwani Kumar Singla, K.S.Sandha — Performance Evaluation of Symmetric Cryptography Algorithms, IJECT, 2011.
4. Diaa Salama, Abdul Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhound — Performance Evaluation of Symmetric Encryption Algorithm —, IJCSNS, 2008
5. Dr. Mohammed M. Alani — Improved DES Security‖, International Multi-Conference On System, Signals and Devices, 2010
6. Tingyuan Nie, Teng Zhang — A Study of DES and Blowfish Encryption Algorithm‖,TENCON, 2009
7. Afaf M. Ali Al- Neaimi, Rehab F. Hassan — New Approach for Modified Blowfish Algorithm Using 4 – States Keys‖ , The 5th International Conference On Information Technology,2011
8. J.Orlin Grabbe —The DES Algorithm Illustrated‖
9. Dhanraj, C.Nandini, and Mohd Tajuddin — An Enhanced Approch for Secret Key Algorithm based on Data Encryption Standard‖, International Journal of Research And Review in Computer Science, August 2011
10. Gurjeevan Singh, Ashwani Kumar, K.S. Sandha —A Study of New Trends in Blowfish Algorithm ‖, International Journal of Engineering Research and Application,2011
11. W. Stallings, Cryptography and Network Security: Principles and Practices, 5th ed., Prentice Hall, 1999.
12. B.Scheier, Applied Cryptography : Protocols, Algorithms and Source Code in C,2nd ed.., John Wiley & Sons, 19995.