Hardware Implementation of the Data Encryption Standard (DES)

W. SANAYHA, Y. RANGSANSERI
Department of Telecommunications Engineering, Faculty of Engineering
King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520
THAILAND

Abstract: - This paper presents hardware implementation of the data encryption and decryption of the DES standard algorithm. The design consists of the S-Box circuit Exclusive-OR circuit, Circular Left Shift circuit and the control unit. The S-Box circuit implemented using 32 PLDs (Programmable Logic Device) chip that hold substitution a 48-bits input data and yields a 32-bits output data. The other circuits implemented using hi-speed CMOS integrated circuits and a PC printer port control the whole operation of the DES. The prototype hardware implementation can produce encrypt and decrypt data up to 30 Mbytes/sec.

Key-Words: - Data Encryption Standard, DES, Hardware Implementation, S-box

1. Introduction

Encryption is a process of encoding a message so that the meaning of the message is not obvious; Decryption is the reverse process: transforming an encrypted message back into its normal form. The original form of a message is known as plaintext, and the encrypted form is called ciphertext. A system for encryption and decryption is called a cryptosystem. Some encryption algorithms use a key, so that the ciphertext, message depends on both the original plaintext message and the key value [1]. This situation is shown in Figure 1.

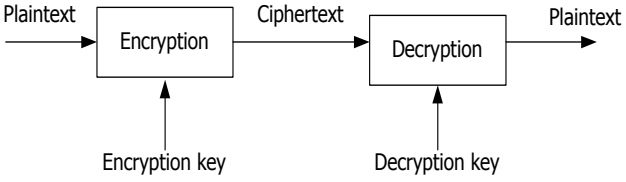

Figure 1: Block Diagram of DES.

2. Data Encryption Standard

The Data Encryption Standard (DES), the well-known symmetric key cipher, was developed due to efforts initiated by the National Security Agency (NSA). In their public request for proposals, where a set of design criteria was specified, the NSA argued that the security of the algorithm must reside in the key. In 1977, DES was adopted as a federal standard for use in commercial and unclassified U.S. government applications. In later years, both hardware and software implementations became widely available. They have been used in many sectors of industry including banking.

2.1 DES Algorithm

DES operates on 64-bit blocks of plaintext to produce 64-bit ciphertext blocks. The length of the encryption key is 56 bits. Since DES is a symmetric cipher, this key is also used for decryption. DES keys are generated as 64-bit number, but in each key every eighth bit is used for error (parity) checking [2]. The DES algorithm is shown in Figure 2

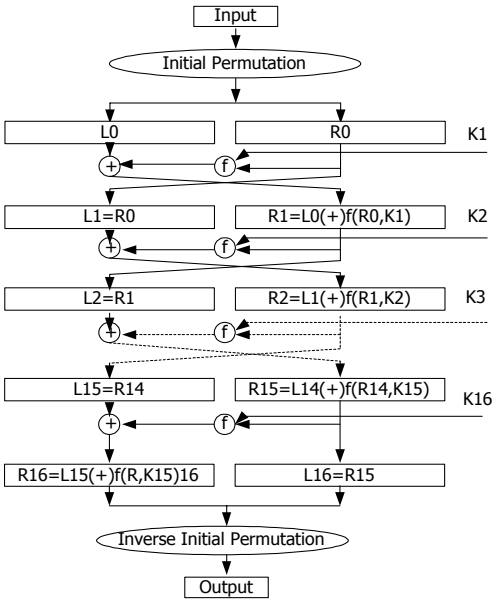

Figure 2: DES algorithm.

The initial permutation transposes the 64-bit block of plaintext as described in IP table. After an initial permutation, the block is broken into a right half and a left half, each 32 bits long. Then there are 16 rounds of identical operations, called Function f, in which the data are combined with the key. After the sixteenth round, the right and left halves are joined, and a final permutation (the inverse of the initial permutation) finishes of the algorithm [3].

2.2 Function *f*

A combination of substitution and transposition operations define the function *f*. The decryption process is just the reverse operation [2]. This process is shown in Figure 3.

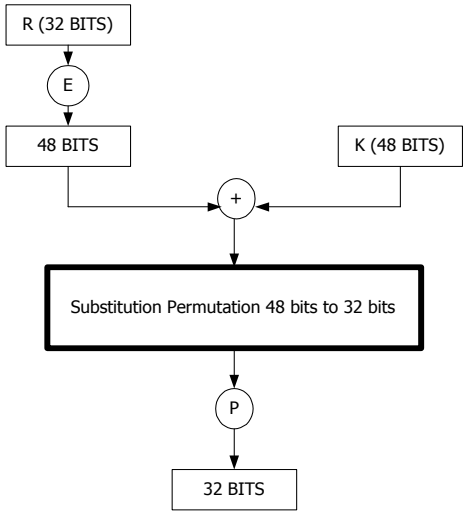

Figure 3: Detail of Function *f*.

Each cycle of the algorithm is really four separate operations. First a right half is expanded from 32 bits to 48 via an expansion permutation. Then it is combined with 48 bits of a shifted and permuted key via an XOR, sent through 8 S-boxes producing 32 new bits, and permuted again. This four operations make up Function f. The output of Function f is then combined with the left half via another XOR. The result of this operations becomes the new right half; the old right half becomes the new left half. These operations are repeated 16 times, making 16 rounds of DES [4].

2.3 S-boxes Permutation

After the compressed key is XORed with the expanded block, the 48-bit result moves to a substitution operation. The substitutions are performed by eight substitution boxes, or S-boxes. The 48 bits are divided into eight 6-bit sub-blocks. Each separate block is operated on by a separate S-box: The first block is operated on by S-box 1, the second block is operate on by S-box 2, and so on, as shown in Figure 4.

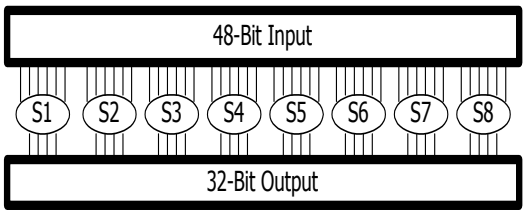

Figure 4: Calculation detail of S-box algorithm.

Each S-box is a table of 4 rows and 16 columns. Each entry in the box is a 4-bit number. The 6 input bits of the S-box specify under which row and column number to look for the output. Table 1 shows an example of S-box 1. It is a table by which six bits of data are replaced by four bits.

Suppose that block is the six bits $b_1\ b_2\ b_3\ b_4\ b_5\ b_6$. Bits b_1 and b_6 , taken together, form a two-bit binary number $b_1\ b_6$, have a decimal value from 0 to 3. Call this value r. Bits b_2, b_3, b_4 and b_5 taken together form a four-bit binary number $b_2\ b_3\ b_4\ b_5$, having a decimal value from 0 to 15. Call this value c. The substitutions from the S-boxes transform each 6-bit block into the 4-bit result shown in row r, column c of section S of Table $\mathbf{S_1}$.

Table 1: S-box 1.

Row No.	Column No.															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Each of the unique selection functions $\mathbf{S_1, S_2, ..., S_8}$, takes a 6-bit block as input and yields a 4-bit block as output and is illustrated by using a table containing the recommended $\mathbf{S_1}$

2.4 Key Transformation

Initial, the 64-bit DES key is reduced to a 56-bit key by ignoring every eighth bit. These bits can be used as parity check to ensure the key is error-free. After the 56-bit key is extracted, a different 48-bit subkey

is generated for each of the 16 rounds of DES. These subkeys, K_b are determined in the following manner.

First, the 56-bit key is divided into two 28-bit halves. Then, the halves are circularly shifted left by either one or two bits, depending on the round. Number of key bits shifted per round is defined in table. Then, the halves are pasted together again, and 48 of these 56 bits are permuted to use as a key during this cycle (see Figure 5).

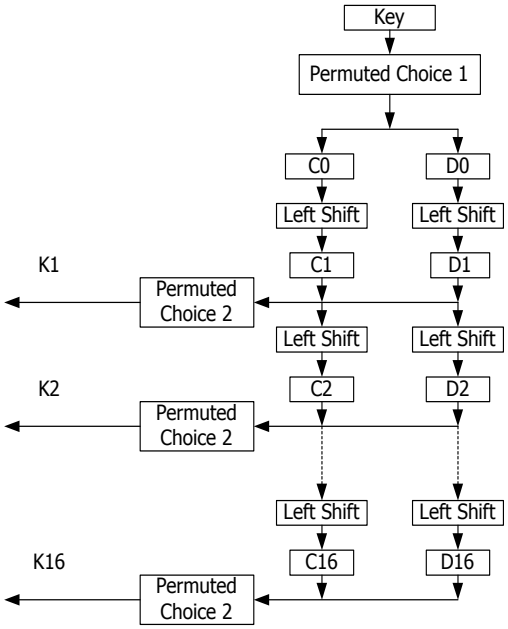

Figure 5: Key schedule calculation.

The key for the cycle is combined by an exclusive-or function with the expanded right half from the section above. That result moves into the S-boxes. At each cycle, the halves of the key are independently shifted left circularly by a specified number of bit positions.

3. Hardware Implementation

3.1 S-Boxes

Hardware design of the DES are separated into two sections. These are data algorithm and key transformation. Permutation and expansion are implemented by hardware wiring. Main of hardware implementation is S-boxes, designed by using PLD (Programmable Logic Device) chip. One PLD chip is programmed output data in a row of the S-boxes table. Thus 6-bit input is passed each $\mathbf{S_1,S_2,...,S_8}$ block yields 4 bits output (see Figure 6).

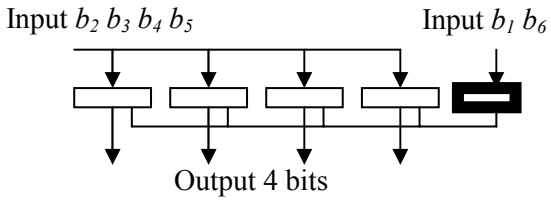

Figure 6: Hardware design of S-box.

Implementation 48-bit input block yields 32-bit output block S-boxes **(S_1, S_2, ..., S_8)** use 32 PLD chips that programmed 32 row of data according to table of S-box.

Group of 4-PLD chips are controlled by a data selector chip that only one PLD chip yields 4-bit output. Whole system of S-boxes shown in Figure 7.

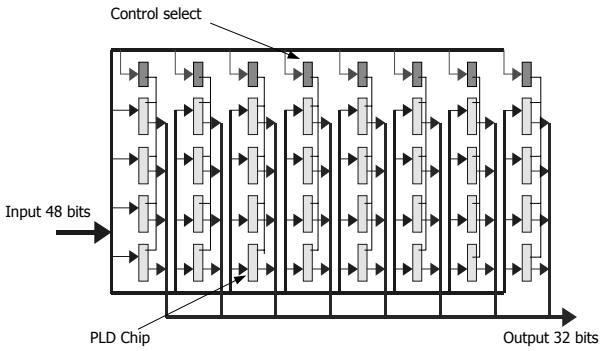

Figure 7: Diagram of the S-boxes system.

3.2 XOR Combination

XOR combination of the DES algorithm have two types, these are 32 bits and 48 bits XOR combination. XOR blocks are implemented by IC chip. Each chip takes a 4-bit block as input and yields a 4-bit block as output. Thus 32-bit XOR combination block will be implemented by 8 IC chips and 48-bit XOR combination block were implemented by 12 IC chips.

3.3 Key Transformation

Key schedule calculation is designed in each part. Generating 64-bit input key from PC, receiving 64-bit input key and Permuted choice 1(PC1), and finally part is circular Left Shift circuit.
Keying 64-bit input is implemented by programming with C++ language method. This part will receive 64-bit input key, then send to receiving key part.

Receiving key is designed by using Microcontroller chip. This chip will be programmed data of Permuted Choice 1(PC1) in its. Microcontroller chip receives 28-bit input and substitutes 28-bit input yields 28-bit output followings PC1 table.

The circular left shift circuit is designed by using IC chip, called Shift Register. These are 4-Bit Bidirectional Universal Shift Register type. It can operate either circular left or right shift. Each chip can receive 4-bit input key. Then, a 28-bit shifting are designed by using 7 IC chips.

3.4 Cycle Control Circuit

The DES algorithm consists of 16 cycles. Hardware implementation must design buffer or latch and control circuit that can control operation of 16 iteration cycles. These are two parts of cycle control circuit. First, data selector circuit is designed by Quadruple 2-Line-to-1-Line Data Selector/ Multiplexer chip.

Finally, data buffer circuit is designed by using CMOS IC chip which have 8 D Flip-Flops in its. Both of circuits can control input and output data that can operate 16 times of iteration cycles (see Figure 8).

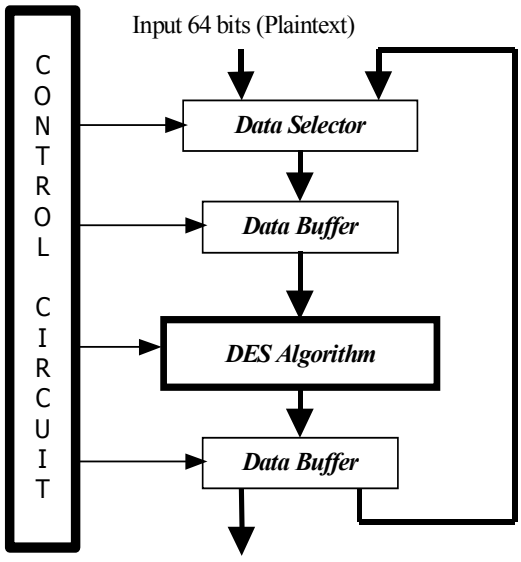

Figure 8: Diagram of the cycle control circuit.

4. Conclusions

In this paper, we have presented designing of the DES hardware that implemented by IC chip device. It can completely encrypt cleartext and decrypts ciphertext. Testing is done by send input data (plaintext) to encryption unit. Then, output of encryption unit is connected to input of decryption unit. After output from decryption unit is measured encryption/decryption rate. Testing result shows encryption/decryption rate at optimum speed (30 Mbytes/sec) because of delay time in internal IC chip device.

Acknowledgment:
This work has been supported by Assistant Professor Dr.Krerkchai Thongnu and Department of Electrical Engineering, Faculty of Engineering, Prince of Songkhla University.

References:

[1] C.P. Pfleeger, *Security in Computing.* Englewood Cliffs, NJ: Prentice-Hall, 1989.

[2] A. Eslicioglu and L. Litwin, Cryptography, *IEEE Potentials,* Volume: 20 Issue: 1, pp. 36-38, Feb-March 2001.

[3] National Institute of Standards and Technology, *Data Encryption Standard (DES)*, FIPS 46-2, USA, 1993.

[4] B. Schneier, *Applied Cryptography: Protocols, Algorithms and Source Code in C.* 2nd ed. New York : John Wiley & Sons, Inc., 1996.