2010 International Conference on Multimedia Communications

Function Modular design of the DES encryption system based on reversible logic gates

Yiqing Zhang
School of Science,
Nantong University,
Nantong, China (226019)
e-mail: Zhang.yq@ntu.edu.cn

Zhijin Guan
College of Computer Sci. and Tech.,
Nantong University,
Nantong, China (226019)
e-mail: guan_zj@nuaa.edu.cn

Zhilang Nie
College of Computer Sci. and Tech.,
Nantong University,
Nantong, China (226019)
e-mail: 0713042051@jsjxy.ntu.edu.cn

Abstract—**Encryption system demands not only high security but low power consumption. Reversible logic arose more and more attention in the recent past due to its less heat dissipating characteristics. This paper analysis the functional module of DES system, then presented a 4:1 mux based on reversible logic gates, and designed respectively a reversible circuit of a 4-bit counter and a reversible circuit of two-way shift register. By using a series of reversible device, we realized the design of reversible circuits for the functional modules.**

Keywords-reversible logic gates; DES; Encryption system

I. INTRODUCTION

DES encryption algorithm is so far the most widely used proprietary encryption algorithm, usually be divided into hardware form and software form, although the process of software encryption/decryption is convenient and has flexible design, but which have large Computation, low speed and the security also can not be guaranteed. The encryption/decryption of the hardware with characteristics of high speed, high reliability and so on. So it can be used in intelligent cards, mobile phones, wireless sensors and other mobile devices. These mobile devices have rigor requirements on the power. Thus, it has great significance on research how to design low-power encryption system.

Landauer [3] have shown that for irreversible logic computations, each bit of information lost, generates $kT\ln^2$ joules of heat energy, where k is Boltzmann's constant and T the absolute temperature at which computation is performed. The energy consumption of traditional circuit is caused by irreversibility of the calculation, if the factors of materials and crafts are not considered. Bennett [4] showed that $kT\ln^2$ energy dissipation would not occur, if a computation is carried out in a reversible way, since the amount of energy dissipated in a system bears a direct relationship to the number of bits erased during computation. Reversible computation in a system can be performed only when the system comprises of reversible gates. Reversible logic operation do not lose information and has very little heat consumption. Thus, the DES encryption system, which is composed of circuit module designed by reversible logic gate can greatly reduce system power consumption.

II. BASIC THEORY

A. DES algorithm

DES algorithm is a sort of grouping encryption algorithm, introduced by IBM , which uses 56-bit key data to operate the 64-bit data module and can fast encrypt a large amount of data at the same time [2][5]. Figure 1 gives the schematic diagram for the algorithm. The encryption process can be summarized as three steps:

(1) Initial permutation. Input 64-bit plaintext, through the initial permutation, it is divided into two parts of 32 bits, they can be recorded as L_0 and R_0 respectively.

(2) A consecutive calculation of 16 rounds. The 32-bit data R_{i-1} and 48-bit key K_i first pass through encryption function $f(R_{i-1}, K_i)$, then the output date and L_{i-1} modulo 2 adders (XOR), at last, we obtained R_i , and R_{i-1} replace R_i of next round , $0 < i <= 16$ .The outputs of left and right part connect into a 64-bit serial number.

(3) An inverse initial permutation. One ciphertext is obtained after a 64-bit serial number inverse initial permutation.

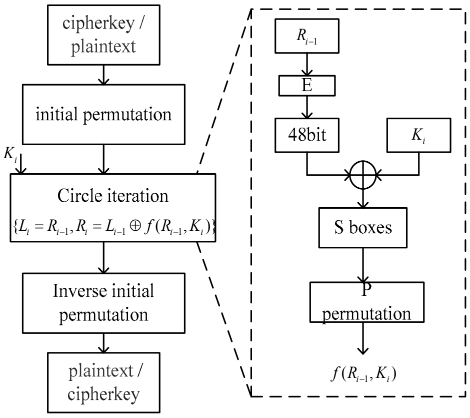

Figure 1. DES algorithm schematic chart

978-0-7695-4136-5/10 $26.00 © 2010 IEEE
DOI 10.1109/MEDIACOM.2010.18

B. Circuit analysis and design

Reversible logic gate is a sort of logic unit which has the same number of input and output, and the input vector and output vector are mapping each other. The existing reversible gates include Feynman gate [6], Toffoli gate [7], as well as Fredkin gate [8]. Figure 2 shows the logic form of these gates.

Literature [1] gives several circuits cascade by some general reversible logic gates. Figure 3 shows the reversible design of the positive edge triggered D Flip-Flop, which is composed of two D flip-latch. If Q^n denotes the current state of the Flip-Flop and *D* is the input signal, the Sub-state of the flip-flop will be $Q^{n+1} = D$ after the positive edge arrive; otherwise, it will be $Q^{n+1} = Q^n$. A simple reversible circuit design of 4-bit shift register can be constituted, if four D flip-flop showed in Figure 3 be cascade and controlled by the same clock pulse.

Literature [1] gives several circuits cascaded by some general reversible logic gates. Figure 3 shows the reversible design of the positive edge triggered D Flip-Flop, which is composed of two D flip-latch. If Q^n denotes the current state of the Flip-Flop and *D* is the input signal, the Sub-state of the flip-flop will be $Q^{n+1} = D$ after the positive edge arrive; otherwise, it will be $Q^{n+1} = Q^n$. A simple reversible circuit design of 4-bit shift register can be constituted, if four D flip-flop showed in Figure 3 be cascade and controlled by the same clock pulse.

Suppose $D = T\bar{Q} + \bar{T}Q = T \oplus Q$, then the reversible circuit design of T Flip-Flop can be realized if a XOR gate is added in front of D input terminal. Figure 4 gives the reversible circuit structure of such T flip-flop. In Figure 5, black solid point stands for a Fey gate (b is set as constant 0) which copies input signal. Other figures are the same case.

In this paper constructs a sort of reversible circuit of 4:1 mux. As shown in Figure 5, it is composed by five Fredkin gates and a Feynman gate. When the enabled port effect, S_0S_1=00,01,10, 11 respectively dominate the control bit of the first, third and fifth Fredkin gate(The Fredkin gates here are controlled by 0), to determine which way is the corresponding output data. Table 1 gives the function table of this reversible mux.

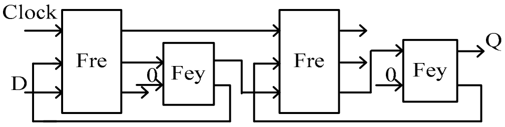

Figure 3. Reversible design of D Flip-Flop

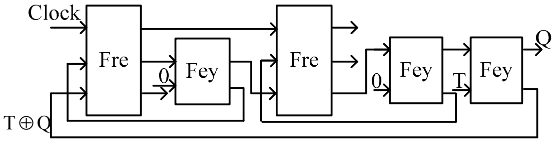

Figure 4. Reversible T flip-flop

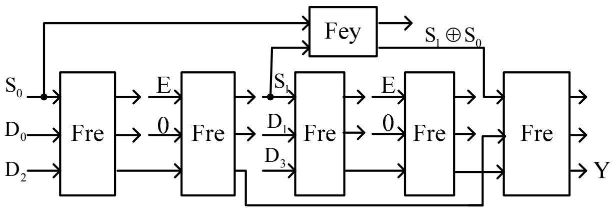

Figure 5. Reversible circuit of 4:1 mux

TABLE I. THE REVERSIBLE DESIGN OF 4:1 MUX

Enabled port	**address**		**output**
E	S_0	S_1	*Y*
0	×	×	0
1	0	0	D_0
1	0	1	D_3
1	1	0	D_1
1	1	1	D_2

TABLE II THE STATE OF 2-BIT COUNTER BASED ON REVERSIBLE GATE

signal	**state**
00	idle
01	input
10	Iteration of 16 rounds
11	output

III. REVERSIBLE LOGIC FUNCTION MODULAR DESIGN OF THE DES

The DES encryption system circuit has three parts: main control module, cipherkey module and operation module.

A. The reversible design of main control module

The main control module is composed of finite state machine and the decoding logic unit. The finite state machine produce state signal to control the state of key module and operation module. We realize four states in Table 2 by using 2-bit counter based on reversible gate.

Encryption process as an example, the conversion process of the state are as follows:

(1) The initial state of circuit is idle, when the initial signal appear a positive pulse, the circuit began to run. It received cipherkey and plaintext, and counter start counting from 0 at the same time. After the cipherkey and plaintext is received at a time, counter plus 1.

(2) When counter=1000, the cipherkey and plaintext have been input 8 times. Since there are 8-bit inputs each circle, the encryption circuit have completed the input of 64-bit plaintext and cipherkey, then a consecutive calculation of 16 rounds can bee started. Counter again began counting from 0, after one round calculation is completed at a time, counter plus 1.

(3) When counter=1111, the circuit have completed the consecutive calculation of 16 rounds, and shift to output state. Counter count from 0.

(4) When counter=00111，the circuit has output the 64-bit inverse initial permutation data.

DES encryption system has two types of work mode, which are encryption and decryption. According to the different work patterns and working conditions, the decoding logic unit generate the corresponding control signals to control the working of key module and operation module. To some extent, this way reduced the power consumption of the chip circuit. Figure 7 shows the reversible design of the main control module.

B. The reversible design of the key module

Under the control of the main control module, the key modules receive the initial key which comes from the external circuit, and generate the sub-key that is needed for encryption and decryption. First of all, we need receive the key. The input key is also 64 bit, but 8 bits are used for parity checking, so there are only 56-bit effective key in initial key. We can use the reversible shift register of 56-bit length, which receive 8-bit data every time in 8 clock cycles and discard the highest bit in each cycle.

Then, one subkey is obtained in control of the main control module. This process can be divided into three parts: permutation selection, left or right shifting cycle and selection permutation. Here the process of permutation is a linear change, which can be realized by connecting lines; when encrypted, left shifting cycle is needed for the key, when decrypted, right shifting cycle is needed for the key.

From the above discussion, we can see that the design of the key module can be realized through the shift register, and because encryption and decryption come down to two-way choice of left shift and right shift, this paper propose a two-way shift register based on reversible gates, as shown in Figure 8. Table 3 gives the function table of this two-way shift register based on reversible gates. Figure 9 shows the reversible design of the key module.

TABLE III FUNCTION TABLE OF THE TWO-WAY SHIFT REGISTER BASED ON REVERSIBLE GATES

Control signal		function
S_0	S_1	
0	0	hold on
0	1	right shift
1	0	left shift
1	1	Parallel input

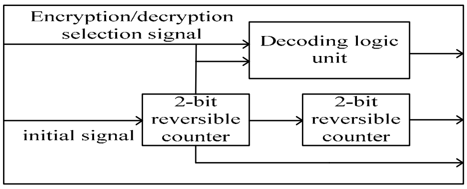

Figure 7. The reversible design of the main control module

C. The reversible design of the operation module

Under the control of the main control module, operation module receive the plaintext or ciphertext and output ciphertext or plaintext after a sequence of initial permutation, cycle iteration and inverse initial permutation through making use of the sub-key generated by the key module. We can use the shift register designed above to receive and send data and use permutation rules to complete initial permutation and inverse initial permutation by the way of connection. The process of iteration operation mainly include an expansion operation E, eight nonlinear substitution functions with six inputs and four outputs (also called *S* boxes) and a permutation P. In this paper, through a Feynman gate, the extension 48-bit data and sub-key modulo 2 adders (XOR). Then the data changed to 32-bit through the transformation of S boxes, at last we get the outputs after P permutation. The expansion operation and P permutation here only need some connection resources. Specific reversible circuit design of operation module is as shown in figure 10.

IV. CONCLUSION

In this paper, we particular analysis the functional modules of DES chip, construct a reversible circuit of 4:1 mux by some general reversible logic gates. On this basis, for every module, we propose reversible circuits of the corresponding device and realize the reversible design of each module. Although in this process, the garbage outputs are increased, owing to reversible logic operations do not lose information bits, therefore the whole system consumes very little heat, and can achieve the design requirements of lower power consumption and smaller size.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China under grant No. 60873069. Doctor foundation of Nantong University under grant No.09B07 and Science and Technology Innovation Program of Jiangsu Province under grant No.081001.

REFERENCES

[1] Siva Kumar Sastry Hari, Shyam Shroff, Sk. Noor Mahammad and V. Kamakoti, “Efficient Building Blocks for Reversible Sequential Circuit Design”, Circuits and Systems, 2006(1): 437-441.

[2] S. B. Ors, “Hardware implementation of a Montgomery modular multiplier in a systolic array”, The 10th Reconfigurable Architectures Workshop (RAW), Nice, France, Apri 2003, l-22.

[3] R. Landauer, “Irreversibility and Heat Generation in the Computational Process”, IBM J. Res. Dev., 1961(5):183-191.

[4] W.C. Athas, L.J. Svensson, J.G. Koller and E. Chou, “Low Power Digital Systems based on Adiabatic-Switching Principles”, IEEE Trans. On VLSI Systems, , April 1994,Vol. 2, No. 4, pp.398-407.

[5] Himanshu Thapliyal, Mark Zwolinski. “Reversible Logic to Cryptographic Hardware: A New Paradigm,Circuits and Systems”, MWSCAS'06. 49th IEEE International Midwest, 2006(1): 342-346.

[6] R. Feynman, “Quantum mechanical computers”, Optics News, , 1985, vol. 11, pp. 11-20.

[7] T. Toffoli, "Reversible computing", Automata, Languages and Programming, 1980, pp. 632-644.

[8] E. Fredkin and T. Toffoli, "Conservative logic", Int'l Journal of Theoretical Physics, 1982, vol. 21, pp. 219-253.

[9] J.D Golic, C Tymen. "Multiplicative Masking and Power Analysis of AES". LNCS: Berlin: Springer-Verlag, 2003, 2523:198-212.

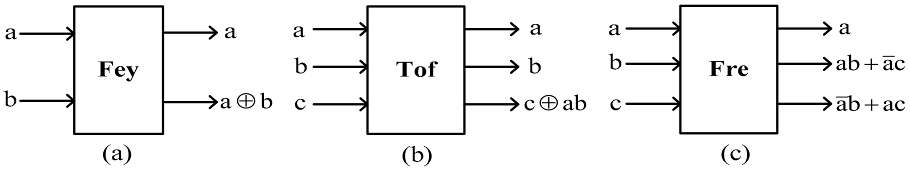

Figure 2. General reversible logic gate: （a）Feynman gate （b）Toffoli gate （c）Fredkin gate

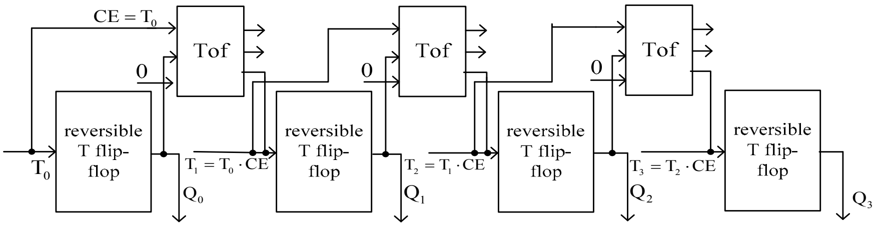

Figure 6. A reversible circuit of 4-bit counter

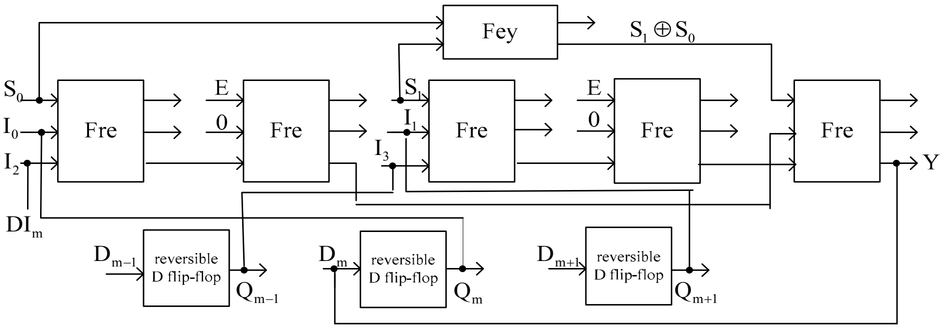

Figure 8. The reversible circuit of two-way shift register

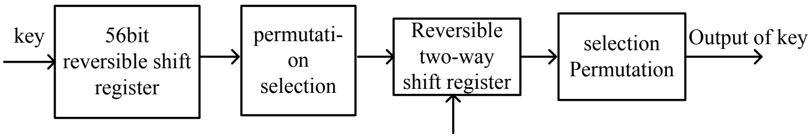
key
56bit reversible shift register
permutati-on selection
Reversible two-way shift register
selection Permutation
Output of key

Figure 9. The reversible design of the key module

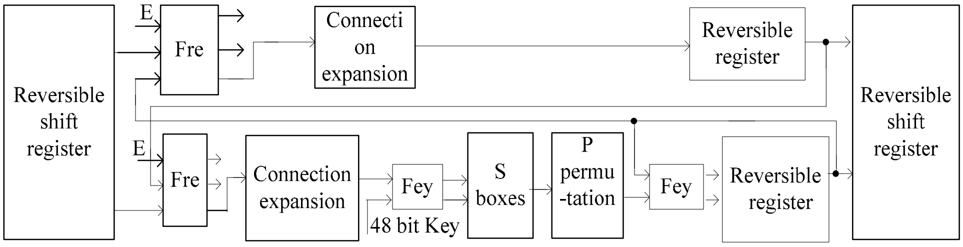

Figure 10. The reversible design of operation module