Security Design of DES Using Reversible Logic

Shikha Kuchhal Rakesh Verma
H.C.E., Sonepat

ABSTRACT
Reversible logic is an emerging research area. Interest in reversible logic is sparked by its applications in several technologies, such as quantum, CMOS, optical and nanotechnology. Reversible implementations are also found in thermodynamics and adiabatic CMOS. Power dissipation in modern technologies is an important issue, and overheating is a serious concern for both manufacturer and customer. One of the main benefits that reversible logic brings is theoretically zero power dissipation in the sense that, independently of underlying technology, irreversibility means heat generation. Synthesis of multiple-output functions has to be done in terms of reversible objects. This usually results in addition of garbage bits which in contrast to the non-reversible case is technologically difficult and expensive. The amount of garbage is a very important criterion for a good synthesis procedure, since in most technologies the addition of only one bit of garbage is very expensive or even impossible to implement. Minimal garbage realization may require a larger number of gates in the circuit, but it is better to have a large but working circuit than a small one that is not ready for the technology. 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. We analysis the functional module of DES system, 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
Encryption, Cryptography, Reversible logic, DES

1. Introduction

We are going to design a circuit for DES using reversible logic. Now question arises i.e. what is cryptography and what is the meaning of reversible logic. Answers to these questions are:
Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet.
Reversible computing is a model of computing where the computational process to some extent is reversible, i.e., time-invertible. A necessary condition for reversibility of a computational model is that the relation of the mapping states of transition functions to their successors should at all times be one-to-one. Reversible computing is generally considered an unconventional form of computing.

2. Data Encryption Standard:

DES is the most popular symmetric-key algorithm. It was standardized in 1977 but expired in 1998. DES is a block cipher, which means that during the encryption process, the plaintext is broken into fixed length blocks and each block is encrypted at the same time. One block is 64 bits and the key is 64 bits wide (but only 56 bits are used).
So we can in a more formally manner describe the algorithm like this:
· _ = _ = { 0,1,2, … ,264-1 }
· _ = { 0,1,2, … ,256-1 }
· each xi has 64 bits
*each key has 56 bits
This description is not complete without the encryption function and the decryption function. The principle of DES encryption is made of an initial permutation, followed by 16 rounds and ended by a final permutation, as we can see in the next figure:
We can see the key-scheduling part at the right which is responsible to give a new 48 bits sub key for each round. Inside each round, the right part of the data is simply swapped while the left part is xored with the result of the f-function applied to the left part.
Now take a closer look at the core of the DES algorithm: the f-function.

Manuscript received September 5, 2015
Manuscript revised September 20, 2015

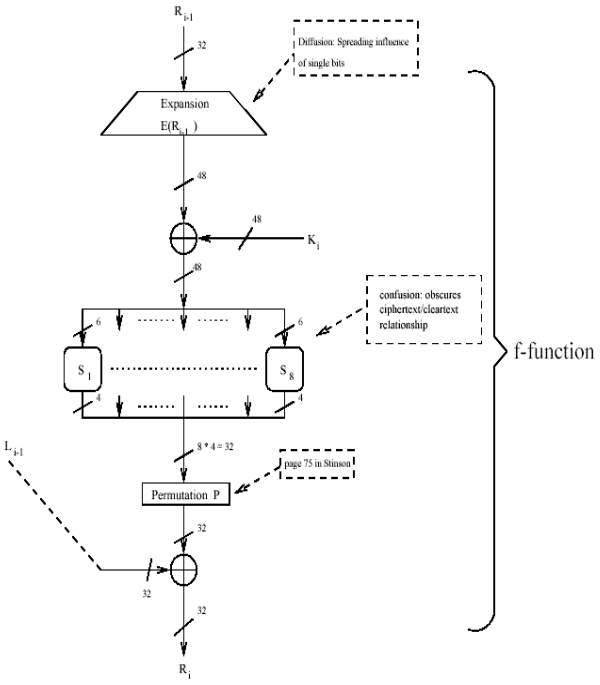

Fig. 1 F-Function

As we can see, the data coming to the f-function goes first through an expansion block and is then xored with the sub key. After that, the data arrives at the S-boxes,which are look-up tables. The next step is a simple permutation and finally, the resulting data is xored with the left part.
At this moment, we must find out how the key-scheduling achieves to build the sub keys.

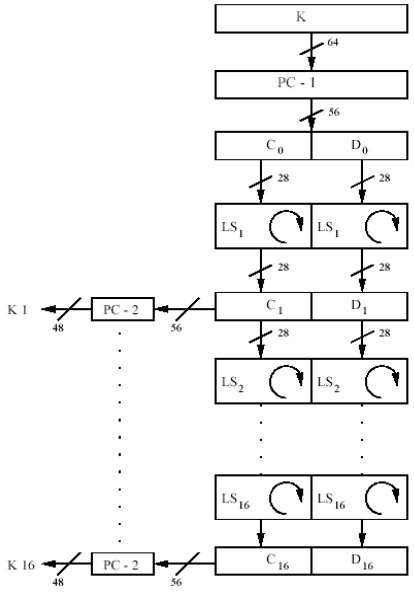

Fig. 2 Key-scheduling

We saw before that the key is initially 64 bits wide. But in the algorithm, only 56 bits are really used. So we can notice in the above figure that the component PC-1 removes these 8 bits to have the correct size. PC-1 also permutes the other bits.
Then, at each step the key is shifted on the left one or two times. Before delivering the sub key, the component PC-2 reduce and permutes the 56 bits shifted key.
Now that we had a good overview of the encryption function (ek), we can take look at the decryption function (dk).
The decryption process is very similar as the encryption one, as we observe in the next schematic:

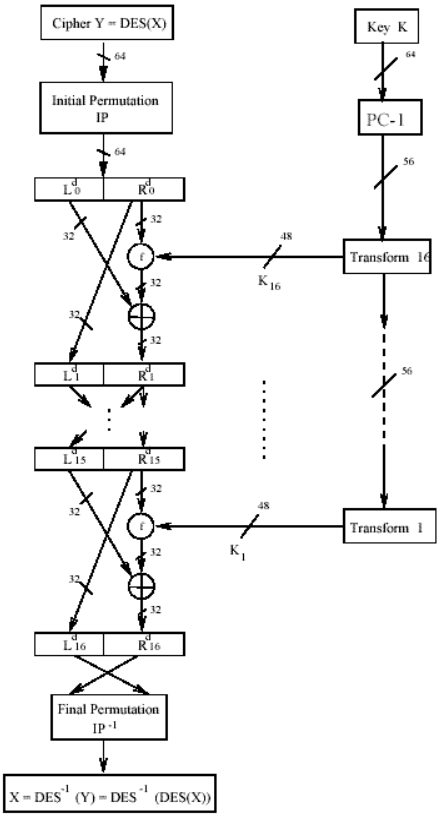

Fig. 3 Decryption

Obviously, the decryption is very similar to the encryption. Only the key-scheduling is reversed. Additionally, we must highlight that there are four standardized modes of operation of DES: ECB (Electronic Codebook mode), CBC (Cipher Block Chaining mode), CFB (Cipher Feedback mode) and OFB (Output Feedback mode). We won't detail all the modes of operation; we just need to know that in our project, we will use the ECB mode, for a detailed description of DES, [2]. In ECB mode, each plaintext block is encrypted independently with the block cipher.

3. Concept and Theory Of Problem

From the literature survey mentioned in the previous chapter, we can conclude that different techniques are available to design reversible logic circuits, From IEEE Paper [1] "Function Modular Design Of The Des Encryption Using Reversible Logic Gates "we can design cryptographic technique using reversible logic

The principle of DES encryption is made of an initial permutation, followed by 16 rounds and ended by a final permutation, as we can see in the next figure:

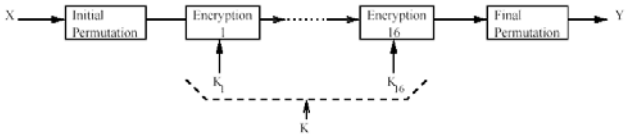

Fig 4 DES block schematic

A more detailed version of this illustration:
The figure below is called the Feistel network. We can see the key-scheduling part at the right which is responsible to give a new 48 bits sub key for each round. Inside each round, the right part of the data is simply swapped while the left part is xored with the result of the f-function applied to the left part.

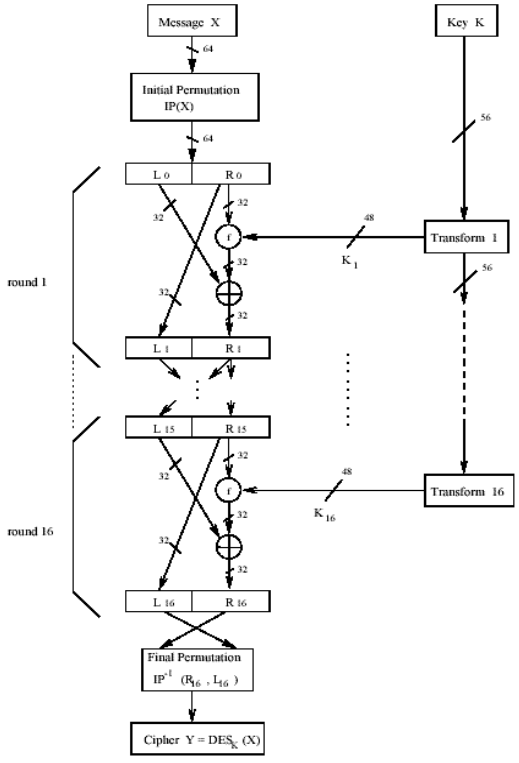

Fig. 5 Feistel network

In our base paper [1] "function modular design of the des encryption using reversible logic gates " there is the proposed design of DES using reversible logic using 4:1 mux, which is a quite complex design to consider. Hence we have implemented the proposed design with reversible counters and register which is much simpler and easy to understand.

4. Result and Discussion

This chapter includes the results of proposed work. The results show the encrypted data with minimum power dissipation as compared with existing circuits. For preparing this work the base paper "Function Modular design of the DES encryption system based on reversible logic gates" was implemented practically using Xilinx software. The proposed circuit for the encryption using reversible logic is as follows:
Fig. 1: Complete distribution of key and operation module.
Fig. 2: Timing diagram of the result with data 11000011.
Fig. 3: Timing diagram of the result with data 11000011.

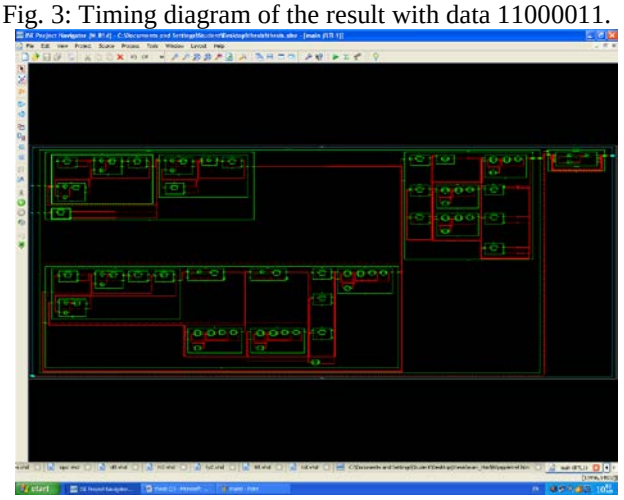

Fig. 6: Complete distribution of key and operation module

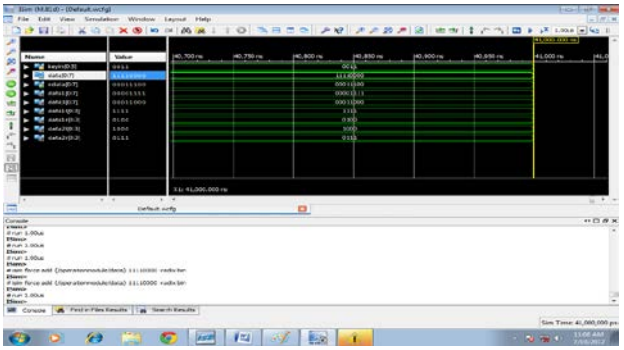

Fig. 7: Timing diagram of the result with data 11000011

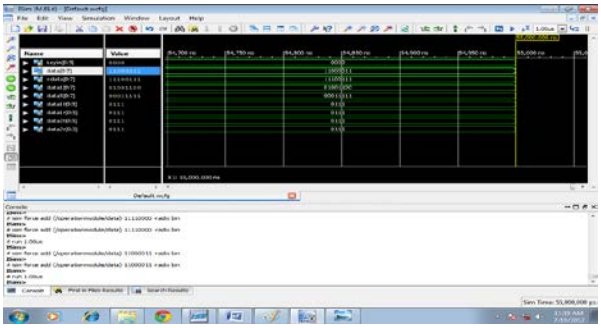

Fig. 8: Timing diagram of the result with data 11000011

5. Conclusion and Future Scope

In these section future aspects for the dissertation has been recommended. That is the properties which can be enhanced in future by applying more efficient implementations or the same implementation more efficiently.

In this dissertation DES algorithm of cryptography is implemented using reversible logic so as to secure data more efficiently with least power consumption.

This dissertation is very enriching, from the course of cryptographic engineering before the beginning of the semester, through the tests with the software's and finally the work at the laboratory with sophisticated tools.

Despite the tests couldn't take place with the logic analyzer, this brought some new knowledge with such professional and interesting equipments.

Some improvements for this project which have been discussed could be applied in future work.

In future work properties like secrecy and integrity in transmission and storage, authentication of identity , threshold systems etc can be enhanced and the circuit can be designed more efficiently using reversible gates having less garbage outputs and less quantum cost. TDES algorithm can also be designed using reversible logic as TDES is more secure cryptographic technique.

REFERENCES

[1] Yiqing Zhang, Zzhijin Guan, Zhilang Nie, "Function Modular Design of The DES Encryption using Reversible Logic Gates",2010,104-107

[2] Wenping Guo, Zhenlog Li, Ying Chen, Xiaoming Zhao, "Security Design For IMS Based On RSA and TDES",2010

[3] Wen Pinn Fang, "VISUAL CRYPTOGRAPHY in Reversible style",

[4] CarlM.Campbell, "Design And Specification of Crytographic Capabilties",1978

[5] P.Kitsos, S.Goudevenos and O.Kouopaulau, "Vlsi Implimentation of TDES Block Cipher",2003,76-79

[6] F.-X. Standaert, G.Rouvroy, J.-JQuiqueter, "FPGA Implimentation of DES and TDES Masked against power Analysis attacks",2006

[7] Hasan Rehan, Sharoj Jamshed,Absar ul hq, "why TDES ith 128 bit key, and not Rijindael should be AES",

[8] Robert Wille, "An Introduction To Reversible Circuit Design", 2011

[9] Efficient ADDER Circuit Based on Reversible Logic Gates

[10] Maryam Ehsaupour, Payman Moallem,Abbas Vafaei, "Design of a novel reversible Multiplier Using Modified Full Adder",2010,V3-230-V3-234

[11] Siva Kumar Sastri Hari,Shyam Shraff , SK Noor Mahammmadand V Kamakoti, "Efficient Building Blocks For Reversible Sequential Circuit Design", circuits and systems,2006,437-441

[12] Stefan frehse, Robert Wille, Raff Drechsle,"Efficient Simulation based Debugging of Reversible Logic",2010,156-161

[13] Yu Pang,Jinzhao Lin, Sayeeda Sultana, Katarzyno Radecka, "A Novel Method Of Synthesizing Reversible Logic",2011,2851-2860

[14] Mozammel H A Khan, Marek Perkowski,"Synthesis Of Reversible Synchronous Counter", 2011, 242-247

[15] New directions in cryptography—invited paper