Implementation of Data Encryption Standard using Reversible Gate Logic

Nuthan.A.C, Nagaraj.C, Havyas.V.B

Abstract*— Cryptography is quite an old art where user can encrypt and decrypt the information using the strongest algorithm which is required for the specific task. But, the scope of this unique information hiding technology has been limited only to the field of software application. Data Encryption Standard (DES) is one of widely used standard for data encryption. Implementation of DES has been done in many ways. But in this proposed implementation, DES is implemented using Reversible logic. Till today not many inventions and growth is observed in reversible logic because of the high complexity in designing them. Reversible logic solutions will be explored to achieve increased levels of power efficiency and area efficiency for digital communication based applications. The modular and flexible nature of the design enables easy incorporation of future updates.

Index Terms*— Reversible logic, Cryptography, Data Encryption Standard (DES).

I. INTRODUCTION

In conventional combinational logic circuits, heat will be dissipated due to every bit transition; hence the information in every bit is lost. Due to this, the information once lost cannot be recovered back. To overcome this problem and to recover the lost bit information, the same circuit is designed using the reversible logic gates. According to Landauer's [1] research, he demonstrated that even with advanced process technology and by using irreversible hardware the circuits and systems can be constructed. He showed the amount of energy dissipated for every irreversible bit operation is given by

$E=KT\ln 2$ Joules ---------- (1)

Where, $K = 1.3806505*10^{-23} m^2 kg^{-2} K^{-1}$ (joule/Kelvin^{-1}) is the Boltzmann's constant

T = Absolute temperature at which operation is performed.

At room temperature, if one bit of information is lost, this yields in low heat generation hence it doesn't affect the performance but in some high computational networks the number of bit lost is more which yields in more heat generation. Hence this will affect the performance of area, speed and power. In Bennett [2] research, he showed that KTln2 joules of energy dissipation in a circuit can be avoided if it is constructed using reversible logic circuits. In both the directions reversible logic gate computes in running process of the system.

The proposed design can be constructed using reversible logic gates because the reversible logic gates will overcome the problems of conventional logic gates, i.e. bit information loss and high power consumption.

II. REVERSIBLE GATES

A reversible logic gate has an equal number of inputs and outputs. Reversible logic is bidirectional hence this can define outputs by inputs and inputs by outputs and also this logic can recover the information of inputs from the outputs. Additional inputs or outputs are added so that the number of inputs is made equal to the number of outputs whenever it is necessary. The number of gates is minimized in reversible logic hence it produce minimum number of garbage outputs.

Several reversible gates have been proposed over the years, e.g., the Toffoli [3] gate, the Fredkin [4] gate etc. Some of the reversible gates are explained in below section.

A. Feynman Gate

Figure 1 shows 2*2 Feynman gate [4] and it is also called as Controlled NOT and it is widely used for fan-out purposes. The input vector is I (A, B) and output vector is O (P, Q). The output is defined by P=A, Q= A ⊕ B. It has Quantum cost of one.

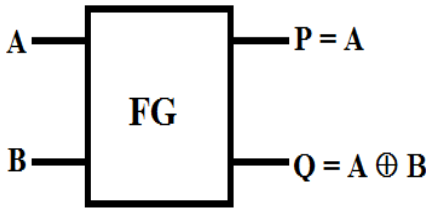

Figure 1: 2*2 Feynman gate

B. Toffoli Gate

Figure 2 shows 3*3 Toffoli [3] gate. The input vector is I (A, B, C) and output vector is O(P, Q, R). The output is defined by P=A, Q=B, R=AB ⊕ C. It has Quantum cost five.

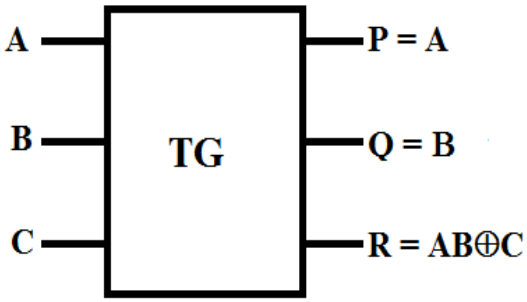

Figure 2: 3*3 Toffoli gate

C. Fredkin Gate

Figure 3 shows a 3*3 Fredkin gate [4]. The input vector is I (A, B, C) and the output vector is O (P, Q, R).

Manuscript Received July, 2013.

Nuthan.A.C, Assistant Professor, Department of Electronics and Communication Engineering, G. Madegowda Institute of Technology, Bharathinagara, Mandya-571422, Karnataka, India.

Nagaraj.C, Assistant Professor, Department of Electronics and Communication Engineering, B.G.S. Institute of Technology, B.G.Nagar, Mandya-571448, Karnataka, India.

Havyas.V.B, PG Student, VLSI Design and Embedded System, B.G.S. Institute of Technology, B.G.Nagar, Mandya-571448, Karnataka, India.

The output is defined by P=A, Q=A'B⊕AC and R=A'C⊕AB. It has a Quantum cost of five.

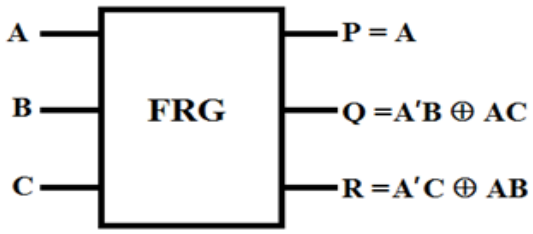

Figure 3: Fredkin gate

III. CRYPTOGRAPHY

The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called codebreaking, although modern cryptography techniques are virtually unbreakable.

As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. Cryptography is used to protect e-mail messages, credit card information, and corporate data. One of the most popular cryptography systems used on the Internet is Pretty Good Privacy because it's effective and free. There exist several cryptography standards in literature. Advanced Encryption Standard (AES) and Data Encryption Standard (DES) etc. are some of examples. In the below section we will discuss Data Encryption Standard (DES).

IV. DATA ENCRYPTION STANDARD (DES)

DES is a secret-key archetypal block cipher with block size of 64 bits. DES encrypts a block of 64-bit plaintext into 64-bit cipher text using 64-bit secret key (Left most bit of a block is bit one). Block diagram of the DES algorithm is shown in the Figure 4.

DES adopted in 1977 by the National Bureau of Standards, now the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46).

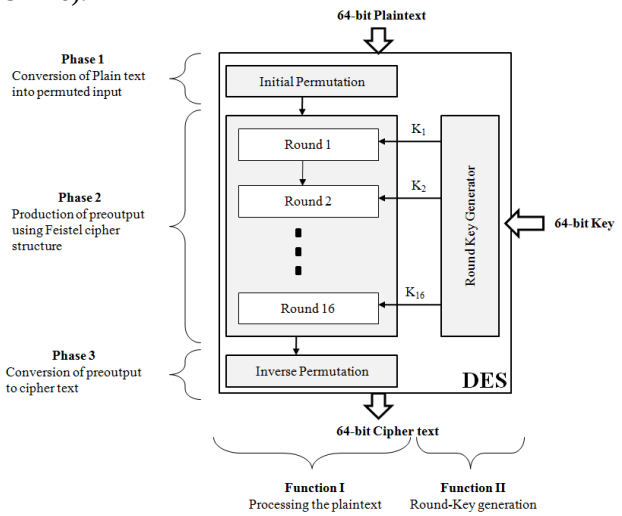

Figure 4: General block diagram of DES algorithm

A DES key consists of 64 binary digits ("0"s or "1"s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, may be used for error detection. The 8 error detecting bits are set to make the parity of each 8-bit byte of the key odd, i.e., there is an odd number of "1"s in each 8-bit byte. A TDEA key consists of three DES keys, which is also referred to as a key bundle. Authorized users of encrypted computer data must have the key that was used to encipher the data in order to decrypt it. The encryption algorithms specified in this standard are commonly known among those using the standard. The cryptographic security of the data depends on the security provided for the key used to encipher and decipher the data.

Data can be recovered from cipher only by using exactly the same key used to encipher it. Unauthorized recipients of the cipher who know the algorithm but do not have the correct key cannot derive the original data algorithmically. However, it may be feasible to determine the key by a brute force "exhaustion attack." Also, anyone who does have the key and the algorithm can easily decipher the cipher and obtain the original data. A standard algorithm based on a secure key thus provides a basis for exchanging encrypted computer data by issuing the key used to encipher it to those authorized to have the data.

DES Encryption process has two functions

A. Processing the plaintext

B. Round-Key generation

A. Processing the plaintext

The processing of plaintext proceeds in three phases.

1. Conversion of Plain text into permuted input
2. Production of preoutput using Feistel cipher structure
3. Conversion of preoutput to cipher text

1. Conversion of Plain text into permuted input

The 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the permuted input, which is split into two 32-bit halves L_0 and R_0 where first 32 bit is L_0 and next 32-bit is R_0.

Permutation is keyless and can be predetermined. This has no cryptographic significance but included to facilitate loading blocks in and out of hardware and to make DES run slower in software.

2. Production of preoutput using Feistel cipher structure

Most symmetric block encryption algorithms are based on Feistel [14] structure. Feistel proposed the use of a cipher that alternates substitutions and permutations which is a practical application of a product cipher that alternates confusion and diffusion functions producing Substitution-Permutation Network (SP Network) [15].

3. Conversion of preoutput to cipher text

The preoutput is passed through a permutation (IP^{-1}) that is the inverse of the initial permutation function, to produce the 64-bit cipher text. This stage has no cryptography significance in DES. The initial and final permutations are straight P-boxes that are inverses of each other.

B. Function 2- Round-Key generation

DES takes 64-bit key as input. Among 64-bit key only 56 bits are effective and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, may be used for error detection or set arbitrarily or can be ignored [13].

The 8 error detecting bits are set to make the parity of each 8-bit byte of the key odd, i.e., there is an odd number of "1"s in each byte. The round-key generator creates sixteen 48-bit round/sub keys out of a 56-bit cipher key. The round key generation block is shown in Figure 5.

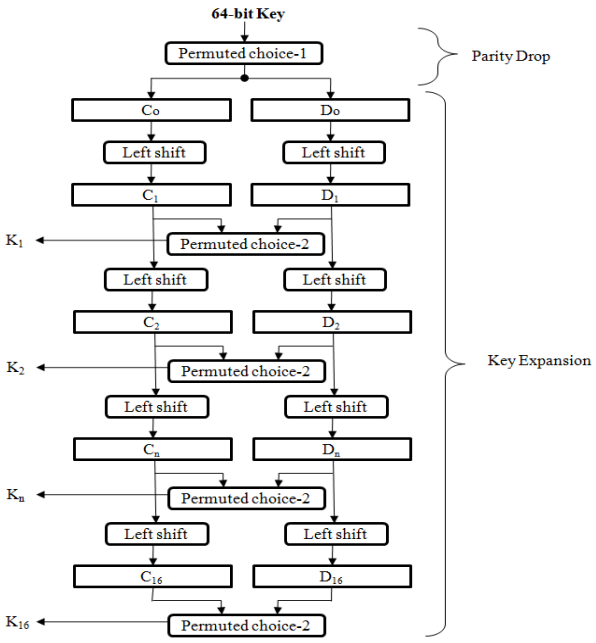

Figure 5: Round Key Generation

V. SIMULATION RESULTS

The entire architecture is modeled using VHSIC hardware description language (VHDL). The coding is done on Xilinx ISE13.2 on Spartan 3 using target device: XC3S400-PQ208 at speed grade of -5. For simulation purpose the Modelsim6.3f has been used. The proposed design can be constructed by using Feynman gate, the Figure 6 shows the top level RTL schematic of proposed data encryption standard with reversible logic gates. The simulation result for data encryption standard using reversible logic gates is shown on Figure 7.

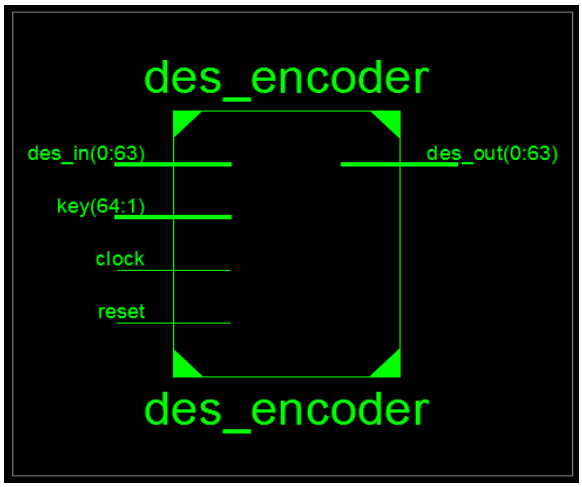

Figure 6: Top level RTL schematic of data encryption standard using reversible logic gates

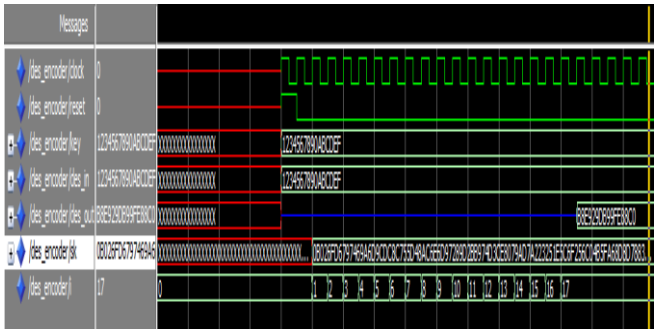

Figure 7: Simulation Results

VI. CONCLUSION AND FUTURE WORK

This paper presents efficient approach for the design of DES using reversible gates. The proposed design can be constructed using Feynman gate. The existing data encryption standard with conventional logic gates will be having bit information loss and high power consumption and in this proposed data encryption standard with reversible logic gates there is no bit information loss and less power consumption compared to the existing data encryption standard with conventional logic gates. The proposed design offers less hardware complexity, less gate count, less garbage bits and constant inputs. In future the same design can be made fault tolerant by making the each sub modules fault tolerant. Since this is implemented on FPGA the same can be efficiently deployed on ASIC in future. The work can be extended to any other cryptic implementations.

REFERENCES

1. R. Landauer, "Irreversibility and heat generation in the computing process", *IBM J. Research and Development*, vol. 5 (3): pp. 183-191, 1961.
2. Bennett, C.H., "Logical reversibility of computation", *IBM J. Research and Development*, vol. 17: pp. 525-532, 1973
3. D. Maslov, G. W. Dueck, and D. M. Miller, "Synthesis of Fredkin-Toffoli reversible networks," *IEEE Trans. VLSI Systems, vol*. 13, no. 6, pp. 765-769, 2005.
4. R. Feynman, "Quantum mechanical computers", *Optical News*, vol. 11, 1985, pp. 11-20.
5. Milburn, Gerard.j., The Feynman processor perseus books 1998
6. E. fredkin, T. Toffoli, "Conservative Logic", *International Journal of Theory of Physics*, 21, 1982, pp 219-253
7. Toffoli T., 1980. Reversible computing, *Tech Memo MIT/LCS/TM-151, MIT Lab for Computer Science.*
8. Michael P. Frank Reversible Computing Page.
9. Carlin Vieri, "Reversible Computing for Energy Efficient and Trustable computation", *April 1998*,
10. P. Picton. Optoelectronic, multivalued, conservative logic. *International Journal of Optical Computing*, 2:19-29, 1991.
11. W. D. Pan and M. Nalasani. Reversible logic. *IEEE Potentials, pages* 38-41, February/March 2005.
12. U.S. Department of Commerce, William M. Daley, Secretary National Institute of Standards and Technology, Raymond G. Kammer, Director, FIPS Pub 46-3 Federal Information Processing Standards Publication Reaffirmed 1999 October 25
13. Cryptography and Network Security Principles and Practices,William Stallings, Fourth Edition.
14. Feistel, H. "Cryptography and Computer Privacy." Scientific American May 1973.
15. Shannon, C. "Communication Theory of Secrecy Systems." Bell Systems Technical Journal, No. 4, and 1949.