INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 6 (2017) PAGES 2407 - 2411
RECEIVED : 25.10.2017 PUBLISHED : 13.11.2017 Nov 13, 2017

An efficient design of reconfigurable reversible gate for data encryption amd decryption

[1]E.Sushma, [2]Syed Noorullah, [3]Madanna
[1]PG Scholar, Dept of VLSI System Design, Geethanajali college of engineering and technology,
[2]Assistant professor, Dept of ECE, Geethanajali college of engineering and technology,
[3]HOD Dept of ECE, Geethanajali college of engineering and technology.

Abstract:
The development in the field of nanometer technology leads to minimize the power consumption of logic circuits. The reversible logic design has been one of the promising technologies gaining greater interest due to less dissipation of heat and low power consumption. On the other hand, energy dissipation in reversible logic gates can decrease to zero. Recently an approach to encryption based on using reversible logic circuits is proposed. This paper presents a solution for designing data encryption and decryption schemes based entirely on reconfigurable reversible logic. In our solution, a building block of encryption and decryption scheme is a cascade of 4-input reversible gates. In this way, the building block can perform any reversible 4-variable function. For this purpose, a reconfigurable reversible logic gate has been proposed.

Keywords: Encryption, Decryption, Reversible circuits, Reconfigurable reversible gate, logic gates.

1. INTRODUCTION

The developing technologies have increased the demand for high-performance computing. According to G. Moore's law, some transistor counts to be integrated per unit area in devices will almost double in one and half year. To accomplish fast computation, high packaging density in the logic circuits is required which brings about more heat dissipation. The conventional computing is found unable to deal with low power, high compaction and heat dissipation issues of the current computing environment. Recently, it is applied to cryptography. A reversible gate is a one-to-one correspondence between its inputs and outputs. Research on reversible logic circuits is motivated by advances in quantum computing, nanotechnology, and low-power design. As a result, reversible logic synthesis has been intensively studied recently.

Application of reversible logic to developing encryption and decryption circuits. The simple implementation of a cipher using reversible logic circuits was the aim of this work. Each gate used in a cascade of reversible gates is determined by the main key. By choosing different main keys, different cascades and different substitution, data encryption and decryption are determined. For this purpose, a reconfigurable reversible logic gate has been proposed. Results of Xilinx ISE based simulation of a simple data encryption and decryption circuits built from reconfigurable reversible logic gates are also presented in the paper. On the other hand, if all a1, a2..., ai coefficients equals one, the gate has negative polarity control lines. These names are obtained after expanding the expressions for the functions realized by the gate. Positive polarity means that all inputs which correspond to control lines directly affect the target line. Negative-polarity means that the target line is affected only if the values of control lines are equal to 0. The

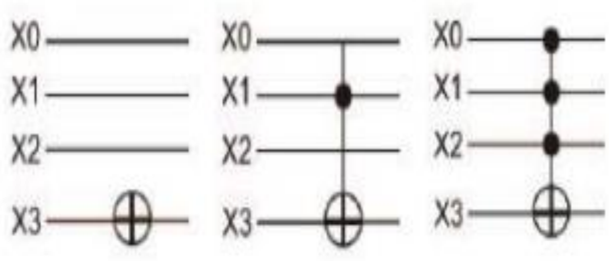

Fig.1.Graphical Representation

term mixed-polarity control lines are used, if all values of the coefficients a1, a2, ..., ai allowed to be either 0 or 1.

2. IMPLEMENTATION

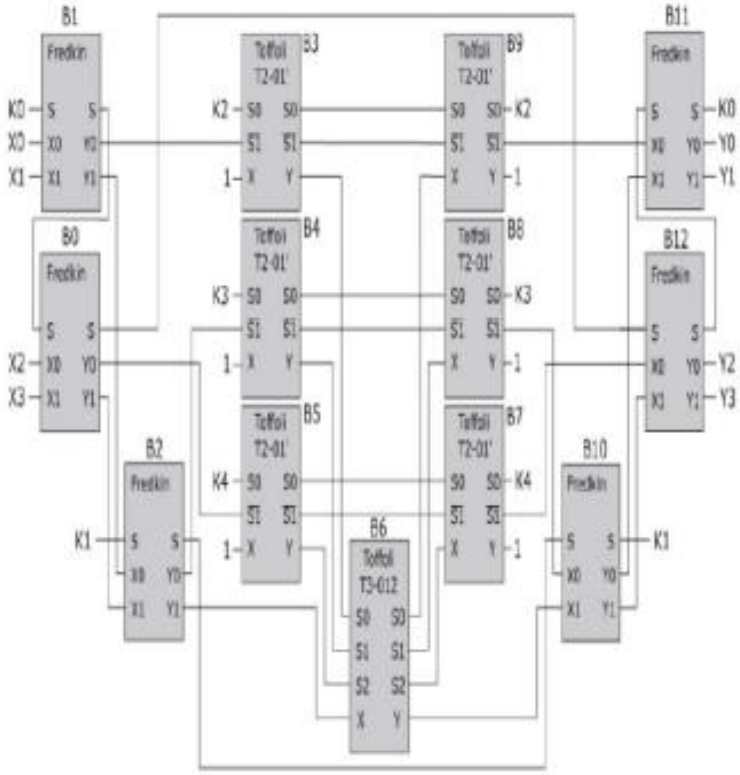

Fig.2. General Structure

At the present state-of-the-art of reversible logic synthesis, it is not possible to optimally synthesize 9-input reversible gate. The first three Fredkin gates B0, B1 and B2 select the input signal which will be modified by the 4- Input Toffoli gate B6. The next three 3-input Toffoli gates B3, B4 and B5 feed control signals for the gate B6 that are selected, by the given configuration either input or constant signals. Thus, the functioning of the gate B6 is determined by signals K. Gates B7, B8 and B9 reconstruct constant signals, while gates B10, B11 and B12 fix the order of output signals Y3, Y2, Y1, and Y0. In the procedure B_NCT signals C1, C2 and C3 determine the number of lines to which control inputs of Toffoli gate are attached while the number of controlled lines is determined by signal C0.

3. RELATED WORK

The basic element of the cipher is a cascade of 16 4-input reversible gates. The same main key is used for data encryption and decryption. The order of gates in the cascade for decryption is reversed in comparison with the cascade for encryption that ensures that it transforms cipher-text into plaintext. hus the circuit shown enables the realization of any 4-variable reversible function.

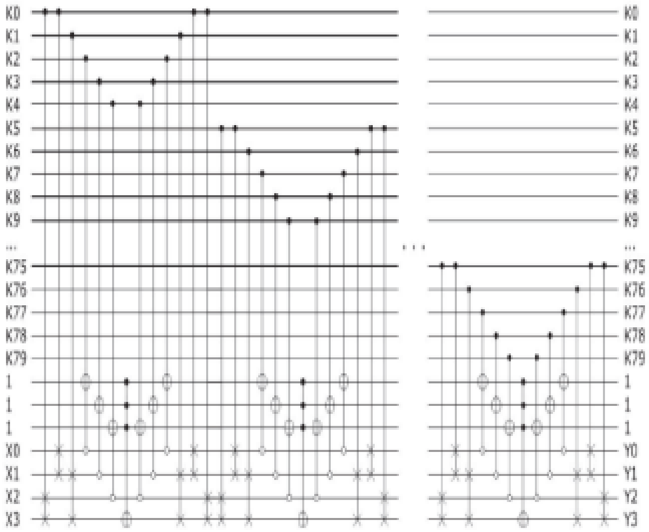

Fig.3. Analysis

The circuit has K which denotes 80 inputs that are partitioned into groups with five inputs in each of them. A 5-line group K [(5*(i+1) – 1):5*i] is used to configure with RRG gate. All inputs K are transferred to outputs so they can be reused for controlling the next gate.There are 4 data inputs X [3:0] and three lines with constant inputs (equal to 1) and equivalent outputs. A detailed description of the main key register, as well as the circuit modifying its contents, during encryption and decryption, are presented in following figures.

4. ANALYSIS

For encryption and decryption, a 5-bit key, two 4-bit ciphers and the main key, a register was used. In this section, first, we will see the synthesis and simulation of the Encryption and Decryption using a reconfigurable reversible gate. Encryption and Decryption using reconfigurable reversible gates are designed on Xilinx ISE 14.7 with Verilog HDL. The RTL schematics and simulation results of the proposed design are shown below. In this way, the building block can perform any reversible 4-variable function. For this purpose, a reconfigurable reversible logic gate has been proposed. The design of such a reconfigurable reversible gate is built from standard reversible gates, i.e., NOT, CNOT, Fredkin and Toffoli gates. This paper presents a complete scheme for data encryption and decryption of 9-bit data using Verilog HDL language.

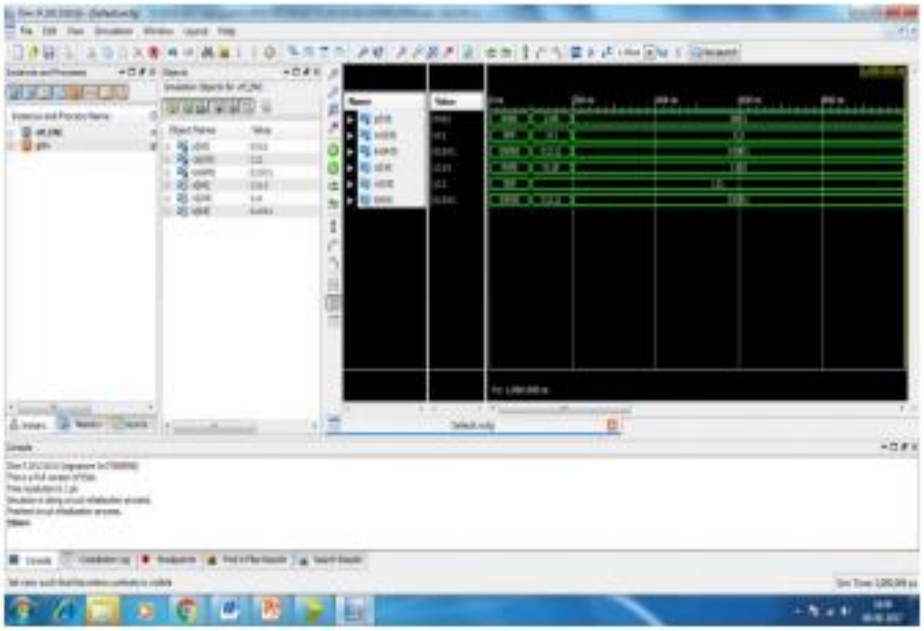

Fig.4. Analysis form

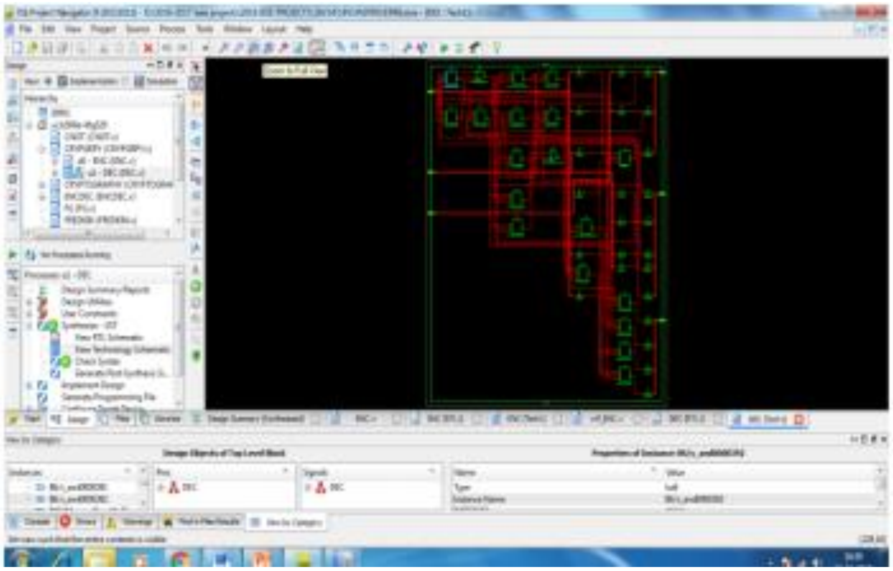

Fig.5. proposed form

CONCLUSION

Firstly, we have coded Verilog code for the reconfigurable reversible data encryption and decryption, and all the synthesis and simulation results are implemented on Xilinx ISE 14.7. The main aim of this paper is a design of simple reconfigurable reversible gate (RRG) which enables implementation of any of the 32 4-input reversible gates from the NCT library. An application of this gate is to implement ciphers for encryption and decryption in the form of binary data. Results of data encryption and decryption simulation of the cipher built from reversible gates are also presented.

REFERENCES

[1] A. De Vos, Reversible Computing. Fundamentals, Quantum Computing, and Applications, 2010.

[2] H. Thapliyal and M. Zwolinski,: "Reversible logic to cryptographic hardware" Proc. 49th International Midwest Conference on Circuits and Systems,2006.

[3] N. M. Nayeem, L. Jamal, and H. M. H. Babu, "Efficiently reversible multiplier and its application to hardware cryptography," Journal of Computer Science, 2009.

[4] Y. Zhang, Z. Guan, and Z. Nie, "Function modular design of DES encryption system based on reversible logic gates," Proc. International Conference on Multimedia Communications, 2010.

[5] A. Banerjee, "Reversible cryptographic hardware with optimized quantum cost and delay," Proc. Annual IEEE India Conference, pp. 1- 4, 2010.