ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

An Advanced Encryption Using Reconfigurable Reversible Logic Gates

P.Anusha
VLSI & ES,
Department of ECE,
Prakasam Engineering College,
Kandukuru, Prakasam Dt, A.P.

Dr.Ch.Ravi Kumar
HOD,
Department of ECE,
Prakasam Engineering College,
Kandukuru, Prakasam Dt, A.P.

Abstract:
Recently, the use of reversible logic circuits based on the encryption / decryption of a policy proposal. The reason for this is that the traditional microscopic techniques are reaching their limits. On the other hand, are theoretically reversible logic circuits with zero power dissipation is reduced. This paper provides a solution for the design of reversible logic entirely based encryption schemes. In our solution, an encryption scheme is a building block for the 4-input cascade of reversible gates. In this way, the building block 4, variable function, which can be reversible. For this purpose, it is proposed a reconfigurable gate reversible. Such a reconfigurable gate gates built from standard reversible, which means that the design, CNOT, Toffoli and Friedkin has been submitted to the gates. The paper in the 8-bit data encryption / decryption of a complete scheme for the VHDL language and its use is described in quantum price is calculated. Simulation and verification of FPGAs in the paper conclude that the scheme. Rijndael encryption system - not an efficient hardware architecture design, and Advanced Encryption Standard (AES) in the current run. The United States National Institute of Standard and Technology (NIST) is defined by the widely adopted AES algorithm. With the development of all the cryptographic algorithms implemented in pure hardware or software can be built. Field Programmable Gate Arrays (FPGA), however, with the help we are to find a swift solution and can be upgraded easily integrate with any treaty changes.

Keywords: Encryption, reversible logic circuits, reconfigurable reversible gate, FPGA.

INTRODUCTION:

Private and confidential data over computer networks, or the Internet, global communications, there is always the data confidentiality, data integrity and availability of the data is likely to be a threat. Data encryption of data confidentiality, integrity and authentication is carried out. Information on the events of daily life, the importance of each of the growing demand for storage has become the most important assets. Messages must be secured from unauthorized party. Encryption is one of the security mechanisms to protect information from public access. To read it except the person who has special knowledge of encryption, so as to make it unreadable to anyone who hides the original content of a message.

The secret keys and encryption, which means that only the use of cryptography in the past, these days, symmetric-key encryption (privet- key cryptography) and asymmetric key encryption (public-key cryptography) and is defined as the different techniques. Public key algorithm is complex and very high computation time. However, public key algorithms two keys, one for encryption and another for decryption private key encryption algorithm with a key only for the two, as well as to have encryption. Such as Data Encryption Standard (DES), 2-DES, 3-DES, elliptic curve cryptography (ECC), Advanced Encryption Standard (AES) cryptographic algorithms and other algorithms have been proposed. Many researchers and hackers are always using brute force and side channel attacks trying to break the algorithm. 1993 [21] and the Data Encryption Standard (DES), as is the case for some of the attacks were successful.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Advanced Encryption Standard (AES) is considered one of the strongest cryptographic algorithms published. The National Institute of Standards and Technology (NIST) Data Encryption Standard (DES) encryption and the collapse of the blocks of data encryption as the standard Advanced Encryption Standard (AES) was adopted. As the draft was published under the FIPS-197 (Federal Information Processing Standard 197) [5]. Moreover, such ATM machines, RFID cards, cell phones and the servers used in many applications. AES extensive real-time audio / video data to be used for encryption of the contents. Due to the importance and the number of applications for real -time of AES algorithm, the main concern of this thesis for the new efficient hardware implementations of the algorithm will be presenting.

AES algorithm is a method in which multiple computation cycles of the algorithm is. A software platform for data, especially high-speed encryption cannot be used for real-time applications. The audio / video content in real-time encryption to trade through video conferencing. Therefore, it is inevitable for applications such as dedicated hardware implementation. The hardware implementation of the area and power consumption, throughput can be done by different forms of trading. At any time, low area and low latency of the best architectural design is a challenge of a special design. AES hardware implementations of the algorithm may vary depending on the application. In some applications, e-commerce servers that require very high throughputs, others as models for cell phones to a medium throughput level.

Some of the others are very small area and low power implementations of the RFID cards need to use the application. The resurrection and the various rounds of the AES algorithm, they Sub Bytes, Shift Rows, Mix Columns and key additional version uses four operations. Sub Bytes transformation is done by S-box. AES S-box speed / throughput is a key part of determining the structure of AES [1]. ROM-based approach requires a large amount of memory and the ROM access time because it causes low latency. Therefore, the arithmetic in the field of composite and S-box (option) for the implementation of VLSI implementation of the AES construction of its hardware optimization is more suitable for the area and it is very important to reduce the power. Custom S-box for AES encryption we created. The logic verification before using the Xilinx ISE FPGA 0.18 µm standard cell library and ASIC technology in both the S-box implementation was carried out by using the VHDL code. Optimization of the design XOR gate and Galois Field (GF) multiplier, the other circuit components, such as small parts, such as has been done by proposing a novel circuit. XOR transistors designed using the minimum and that the high noise margin and much lower power consumption compared to existing designs is XOR.

AES with a module for design optimization done by the restoration of the structure of conventional modules that best suits the area and there is a reduction in the delay. Further, we Xilinx FPGA for implementing AES, namely, resurrection, and both (the pipeline) have synthesized two different design styles. The structure can be realized with a low recurrence Compared to both the structure of the area in which there is a high throughput, but lower throughput. Reversible computing is an emerging area of research. Computer science, there are applications in many areas such as quantum computing, nano-technologies, optical computing, digital signal processing, bioinformatics, and low-power computing [1]. Recently, cryptography [2-10] has been applied. If there is one similarity between the inputs and outputs of a circuit (gate) is reversible.

Research reversible logic circuits for quantum computing, nanotechnology and encouraged development of low-power design. Therefore, reversible logic synthesis has been studied intensively recently. Attention is focused mainly on the synthesis of circuits built from the gates of the NCT library, CNOT and Toffoli gates. Such circuits of modern simulation tools based on FPGAs [11] started modeling.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

VHDL design of a cipher described in [9]. In the paper we study an application of encryption logic circuits to developing reversible. The use of reversible circuits the normal operation of a cipher is the target of this work. Kona reversible gates will determine the key used for each gate. The main keys to choosing a variety of encryption is determined by the different streams and different alternative. For this purpose, it is proposed a reconfigurable gate reversible. The gate is designed to be displayed for the first time in literature. A common method of reversible gates built from the FPGA-based simulation of the circuit also presented the results.

BACKGROUND ON REVERSIBLE LOGIC GATES:

Peres reversible gates of the gate that this work [10], Feynman gate [14], double Peres gate [11], and Toffoli gate, [13] there. Quantum cost is the cost associated with each of the gate is reversible. 1x1 and 2x2 reversible gate of a reversible quantum gates or quantum logic gates [11, 16] No need to design. All reversible 1x1 and 2x2 taken in the unity of quantum gates. As shown in Fig.1 is an example of the gate, the entrance to the 1x1 reversible.

Fig. 1. NOT gate

A. Feynman Gate (CNOT Gate):

Feynman gate (FG) or controlled gate (CNOT) 2 inputs, inputs (a, b), which are mapped to the outputs (P = a movie, Q = A⊕B) 2 outputs is reversible gate. 1. Figures 2a and 2b of the quantum Feynman block diagram of the gate and show a graphical representation. Feynman reversible logic gate widely, either b = 0 in the fan out of the way to avoid the problem when it is used for a copy of the signal, or the signal is used to produce a filler when B = 1.

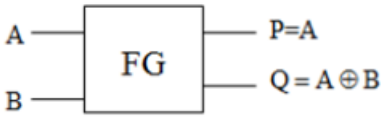

Fig. 2a. Feynman gate

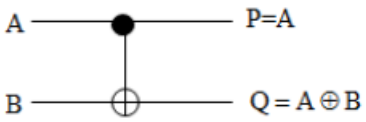

Fig.2b. Graphical representation

B. Peres Gate (PG):

Figures 3a and 3b show the Peres gate and its graphical representation. It is a 3*3 reversible gate having inputs (A, B,C) and outputs P = A, Q = A⊕B, R = AB⊕C. The quantum cost of Peres gate is 4 [10], since it requires 4, 2x2 reversible gates in its design.

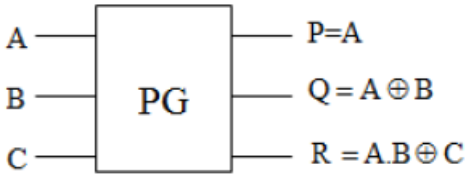

Fig. 3a. Peres gate

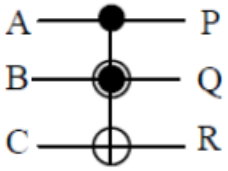

Fig.3b. Graphical representation

C. Toffoli Gate (TG):

Figures 4a and 4b show the Toffoli gate and its graphical representation. It is a 3*3 gate with inputs (A, B, C) and outputs P=A, Q=B, R=AB⊕C. Toffoli gate is one of the most popular reversible gates and its quantum cost is 5. The quantum cost of Toffoli gate is 5 [13] as it needs 5 2x2quantum gates to implement it.

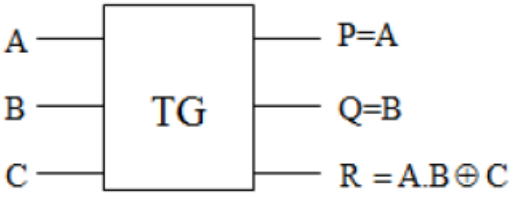

Fig.4a. Toffoli gate

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

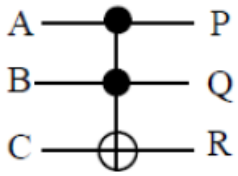

Fig.4b. Graphical representation

D. Double Peres Gate:

Figures 5a and 5b show the block diagram and graphical representation of the Double Peres gate (DPG), respectively. Itis a 4x4 reversible gate with inputs (A, B, C, D) and outputs P=A, Q=B, R=A⊕B⊕D, S=(A⊕B) D⊕(AB⊕C). The quantum cost of DPG is 6 [11], as it requires 6 2x2 quantum gates to implement.

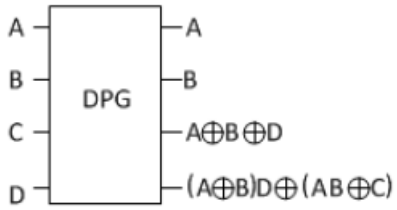

Fig. 5a. Double Peres gate

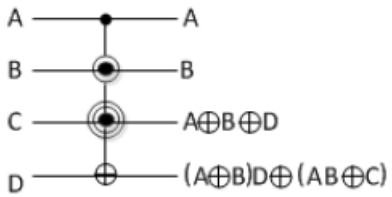

Fig.5b. Graphical representation

PROPOSED QUANTUM CIRCUITRY FOR SQUARE COMPUTATION:

In this section, we are dedicated to the quantum circuit design method to compute the square of the current. The partial product generation unit is reversible and went in the square dedicated to the proposed enhancement will be carried out in phases. For simplicity, we will first present a 4x4 reversible square units. n bit square units will be displayed in the next section. 4-bit partial product generation to the square of the unit shown in Fig. 6. Using the partial product range in relation to the product mix that is equal to some of the terms in the middle section of Fig.6, is shown from the ai • aj + aj • ai = 2 • ai • aj.

The rectangular boxes are used to show equal as possible between the product. After applying the same with regard to the provisions of the relevant product, to increase their weight by 2, so they are shown in the next column. With the addition of a Word to be left arrow shows the position. Fig.6 reduced partial products are in the last part of the last.

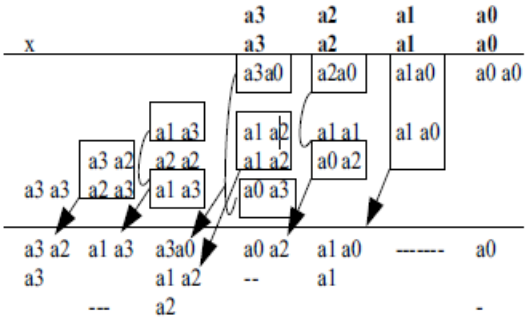

Fig.6. Partial product generation of 4x4 square unit

REVERSIBLE CIRCUIT METRICS CALCULATION FOR N BIT SQUARE UNIT:

4-bit per square unit, reversible design (Fig. 11) can be extended to any size. In this section we like to spend Quantum, ancilla inputs, and outputs n bit crap metrics to assess the current square circuit. n bit square unit, a reduction in the required number of partial products method (as illustrated in the Fig.6) generated using. The most common measurement is calculated using Equation 1 is as shown below. K and L indicate the position of the bit, and n is the number of bits used to represent the value method. The production of a series of partial products can be expressed mathematically

$$a^2 = \sum_{k=0}^{n-1} a_k \bullet 2^{2k} + \sum_{k=0}^{n-2} \sum_{l=k+1}^{n-1} a_k \bullet a_l \bullet 2^{k+l+1} \qquad (1)$$

The estimation of circuit metrics is shown in two steps. In Step 1 only partial products generation circuit is considered and it is generalized for n bit square computation. In Step 2 the complete circuit estimation is discussed.

CONCLUSIONS:

The main aim of the 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. The design of RRG is presented for the first time in the literature. An application of this gate to implement ciphers for encryption and decryption of binary data is described. Results of FPGA-based simulation of the cipher built from reversible gates are also presented.

REFERENCES:

[1] A. De Vos, Reversible Computing. Fundamentals, Quantum Computing, and Applications. Wiley-VCH, Berlin 2010.

[2] H. Thapliyal and M. Zwolinski,: "Reversible logic to cryptographic hardware: a new paradigm," Proc. 49th International Midwest Conference on Circuits and Systems, s. 342-346, 2006.

[3] N. M. Nayeem, L. Jamal , and H. M. H. Babu, "Efficient reversible Montgomery multiplier and its application to hardware cryptography," Journal of Computer Science, vol. 5, no. 1, pp. 49-56,2009.

[4] Y. Zhang, Z. Guan, and Z. Nie, "Function modular design of the DES encryption system based on reversible logic gates," Proc. International Conference on Multimedia Communications, pp. 104-107, 2010.

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

[6] K. Datta and I. Sengupta, "Applications of reversible logic inncryptography and coding theory (Tutorial)," Proc. Conference onVLSI Design (VLSID), 2013.

[7] K. Datta, V.Shrivastav, I. Sengupta and H. Rahaman, "Reversiblelogic implementation of AES algorithm," Proc. 8th International Conference on Design and Technology of Integrated Systems in Nanoscale Era (DTIS), pp. 140-144, 2013.

[8] A.C. Nuthan, C. Nagaraj and V.B. Havyas, "Implementation of Data Encryption Standard Using Reversible Gate Logic," International Journal of Soft Computing and Engineering, vol. 3, no. 3, pp. 270-272, 2013.

[9] A. Skorupski, M. Pawłowski, K. Gracki, and P. Kerntopf, „FPGA based modeling of encryption systems implemented in reversiblelogic" (in Polish), Pomiary Automatyka Kontrola, vol. 58, no. 7, pp.620-622, 2012.

[10] A. Skorupski, M. Pawłowski, K. Gracki, and P. Kerntopf, Reconfiguration of reversible functions using modeling of gates inFPGA" (in Polish), Pomiary Automatyka Kontrola, vol. 60, no. 9, pp.471-473, 2014.

[11] M. Pawłowski and A. Skorupski, Design of Complex Digital Devices(in Polish), WKŁ, Warsaw 2010.

[12] O. Golubitsky and D. Maslov, "A study of optimal 4-bit reversible Toffoli circuits and their synthesis," IEEE Transactions on Computers, vol. 61, no. 9, s. 1341-1353, 2012.

[13] M. Szyprowski and P. Kerntopf, "A Study of Optimal 4-bitReversible Circuit Synthesis from Mixed-Polarity Toffoli Gates,"Proc. 12th IEEE Conference on Nanotechnology, 2012.

[14] M. Bryk, "Cipher built from reversible gates" (in Polish), MSc thesis, Institute of Computer Science, Warsaw University of Technology, February 2016.