Hardware Implementation of RCA Based S-Box for PRESENT Encryption Algorithm

K.J.Jegadish Kumar[#1], B.Partibane[#2], B.Vinodh[*3]

[#]*Assistant Professor,* [*] *PG Scholar, ECE Department*
SSN College of Engineering, Chennai, India.
[1]jegadishKj@ssn.edu.in
[2]partibaneb@ssn.edu.in
[3]vinodh014@gmail.com

Abstract - A design of new block cipher is needed since AES not suitable for resource constraints applications such as RFID tags and sensor networks. In this paper, a cipher called PRESENT encryption algorithm that use cellular automata based S-Box is synthesized and simulated in Altera Cyclone III –EP2C5F256 and Model sim. This leads to reduction in power consumption, area and timing requirement. The block cipher input stream will be 64-bit and 80 or 128 bit key length. The synthesized module is implemented in Altera Quartus Tool and its performance is analyzed. The Power and area is analyzed for PRESENT S-box, AES S-box and Novel Design of PRESENT S-box using Cellular Automata. In major part of the cryptography process more power is consumed by S-box layer, so it's better to optimize performance of this Layer and at the same time security should not to be compromised.

Keywords - **S-Box Substitution, P-Box Permutation, RCA-Rule 30 Cellular Automata, LUT-look up table,**

I. INTRODUCTION

The cryptography plays a vital role in the hardware security application. The major part of the security is hardware and cost factors. The security level depends on the cost of the hardware, but nowadays we come across optimized power and low cost security. The level of cost depends on the hardware consumed and design methodology. In terms of VLSI technology, we will come across design complexity that depends on the internal gates used or LUT applied. To increase the speed of operation we need to complex the design which will increase the slices. This will lead to increase the computation speed that we need as well as power that we doesn't need. So to compensate all parameters we need to go for the modification in design or methodology.

In PRESENT Encryption algorithm the possible outcomes are related to AES. The Security is always a comparable term since level of security changes from one standard to another. And ultimately due to this choice, the encryption standard is varied in terms of power, area, speed and security. The correlation will be there between each parameters and it is difficult to achieve all in determined value. The paper is about comparison of encryption standards particularly using two S-Box. S-Box is the substitution box where the logic is applied. The cipher out is obtained only by transformation in the S-Box and transposition in P-Box through several rounds with key input register. S-Box and P-Box part covers the major part in power consumption and key register increases the security level considerably. So to reduce the power and area the modification to be done here is the S-Box.

To compare the S-Box of PRESENT, original S-Box is replaced with S-Box that is designed based on the concept of Cellular Automata. The purpose of going to the Cellular automata due to its reversibility property particularly in Rule 30 RCA and high parallelism nature.

II. DESCRIPTION OF PRESENT ALGORITHM

A. Substitution Box

In the substitution box 4-bit – 4-bit sub byte transformation, the adverse changes in the output from input depend on the LUT or Logic used in S-Box. The output of the S-Box is given as input to the P- Box which is explained in preceding Part. Here the transposition of S-Box output is made in the Permutation Box. The Sub bytes transformation is a non-linear byte substitution, operating on each of the state bytes independently. The Sub bytes transformation is done using a once precalculated substitution table called S-box [2].

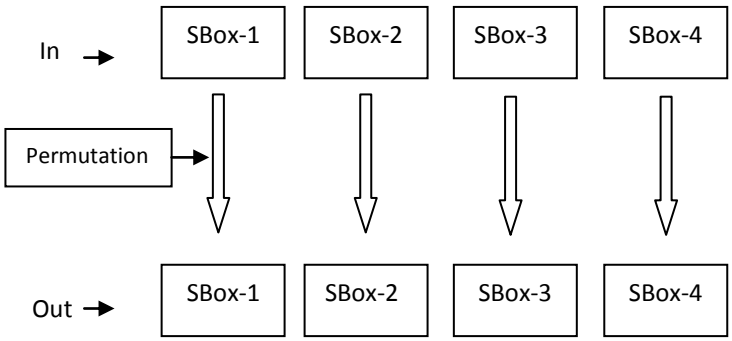

Fig. 1 Substitution Box

B. Permutation Box

In the Permutation layer, the transposition of the S-Box output is done. So the randomness is achieved by passing through various rounds with key register. When choosing the mixing layer, our focus on hardware efficiency demands a linear layer that can be implemented with a minimum number of processing elements, i.e. transistors. This leads us directly to bit permutations. Given our focus on simplicity, we have chosen a regular bit-permutation and this helps to make a clear security analysis [1].

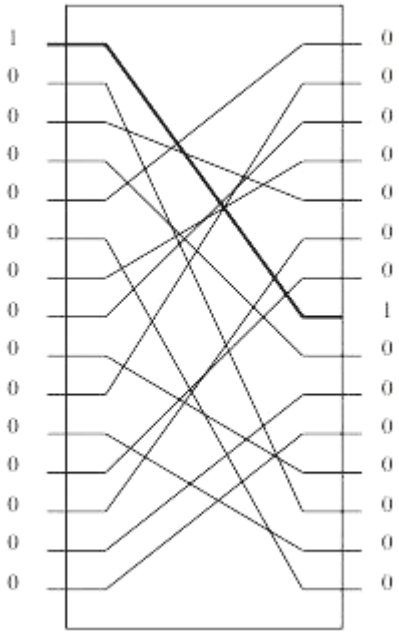

Fig. 2 Permutation Layer [1]

C. SP Network

The output of SP-Network will be the cipher out due to transposition and transformation from input key given. This is achieved by passing updated key through various rounds to Ex-OR with output of P-Box. Here the power consumption is more compared to other layers since slices consumption will be more in this Box. The combination of Substitution and Permutation Network will result in increase the complexity in transition of message bits. The high transition at the permutation layer will result in cipher out. The transition depends on the logic used in designing the SP-Network. The Figure 3 shows the SP-Network topology describes the transition from 4 bit to 4 bit S-Box through the Permutation layer.

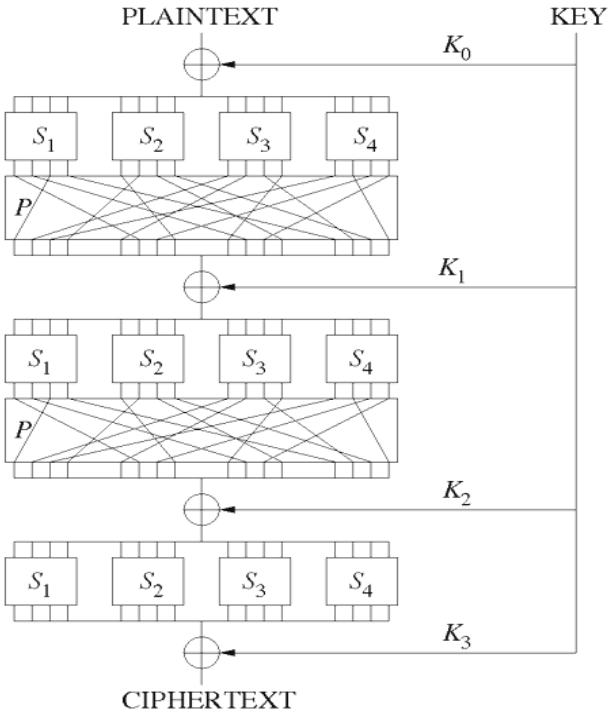

Fig. 3 SP- Network 4bit to 4bit

D. Key Schedule

In PRESENT algorithm, Key length is fixed as 80 bit or 128 bit to reduce the key manipulation attack. Among those 80-bit key is considered as User Specified and Key Stored in Register K. At Round i the 64-Bit Round Key

$K_i = K_6 K_{62} K_{61} \ldots\ldots K_0$ consists of the 64 leftmost bits of the current contents of register K. Thus at round, $K_i = K_{63} K_{62} \ldots\ldots K_0 = K_{79} K_{78} \ldots K_{16}$. After extracting the round key K_i, the key register $K_i = K_{79} K_{78} \ldots\ldots K_0$ is updated as follows.

1. $[K_{79} K_{78} \ldots\ldots K_1] = [K_{18} K_{17} \ldots\ldots K_{20} K_{19}]$ (1)

2. $[K_{79} K_{78} K_{77} K_{76}] = S[K_{79} K_{78} K_{77} K_{76}]$ (2)

3. $[K_{19} K_{18} K_{17} K_{16} K_{15}] = [K_{19} K_{18} K_{17} K_{16} K_{15}] \oplus$ round_counter (3)

Thus, the key register is rotated by 61 bit positions to the left, the left-most four bits are passed through the present S-box, and the round_counter value i is EX-OR ed with bits $[K_{19} K_{18} K_{17} K_{16} K_{15}]$ of K with the least significant bit of round _counter on the right [1].

E. Cipher output

The cipher out is the unrecognized output of SP-Network due to various transformation. At each round the SP-Network output will give cipher out where its proximity is increased considerably. The key plays a major role to decrypt the cipher out. Here finding the original initialized key will be most important to obtain the original message. So the simultaneous encryption and decryption will reduce consumption of area in PRESENT algorithm. The Entire structure for PRESENT Algorithm is shown in figure 4.

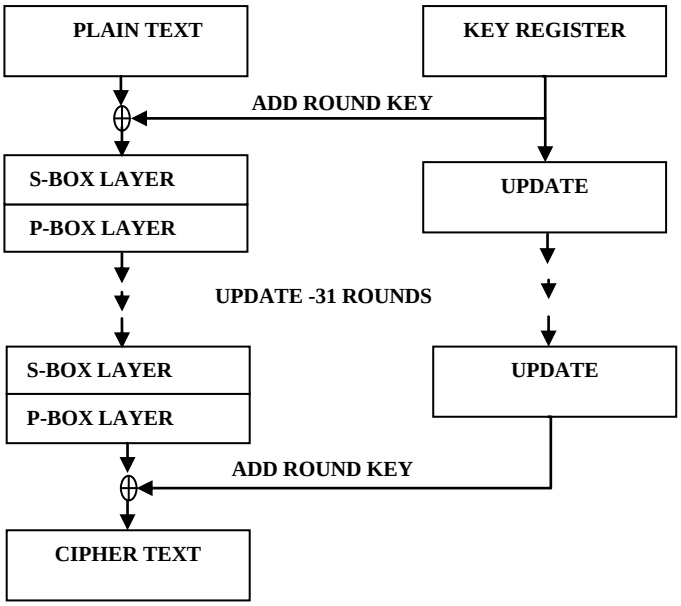

Fig. 4 PRESENT Encryption Algorithm Process Structure

III. S- BOX DESIGN

The New S-box based on the cellular automata is used to modify conventional S-Box of PRESENT Encryption algorithm. The objective of this modification is to optimize the power and area performance and increase the security. Since the maximum power is consumed by the S-Box, so the modification is done in same stage.

A. Cellular Automata

A cellular automaton (CA) is a discrete model studied in computability theory, mathematics, physics, complexity science, theoretical biology and microstructure modelling. It consists of a regular grid of cells, each in one of a finite number of states, such as "On" and "Off". Cellular Automata is the calculation method needs high speed processing of data. Large amount of data must be processed in short time. Speed of operation in implementation is independent of Cellular Automata rule. The purpose of applying CA is to design replicating system that has computationally complex.

The description for the cellular automata is it is a regular lattice of cells, each of which have finite number of states. Cell states are updated in discrete time steps and defined by it's original state and state of cell surrounding it.

Consider the cellular automata is finite array of cell in field f, Cell C= ({0,1} ,f)

Field f => mapping f: {0,1} n → {0,1} – local transition

N => Number of cells the local transition function depends on.

CA => Updates itself with respect to f on each iteration

State of ith cell at time (t+1) depends on state of (i-1)th, ith and (i+1)th cell at time t. Cellular automata are also called cellular spaces, tessellation automata, homogeneous structures, cellular structures, tessellation structures and iterative arrays.

(i) 1-D Cellular Automata

1-D cellular automata consist of row of cells and associated set of rules. Each cell can be in one of several states. Number of possible states depends on the automaton. Cells can change from one state to another state. Cellular automaton rule determines how state changes. The working comes in different criteria i.e., when time comes for the cell to change state each cell look around gathers information from the neighborhood cells. This mapping based on the own state, neighbor's state, rule of CA which implies that cell on its own decide what it's new state should be. All the state changes at the same time. This is shown in figure 5.

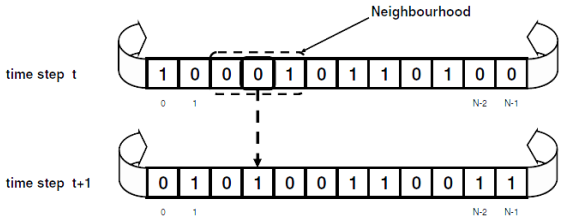

Fig. 5 1-D Cellular Automata

B. RCA Rule -30

In RCA Rule-30, the main advantage is it's reversibility and hence encryption and decryption can be made at the same time. Since the function for the cellular automata itself contains the reversibility function so separate function can be neglected. The LUT for the RCA rule 30 is given in table 1.

Table 1. LUT for RCA Rule-30 S-Box

COUNT	000	001	010	011	100	101	110	111
OUT	0	1	1	1	1	0	0	0

IV.IMPLEMENTATION OF S- BOX DESIGN

A.PRESENT S- Box Design Implementation

The PRESENT algorithm is the base architecture of the encryption. From the flow, the changes made in S-Box design will result in changes in power and security. S-Box for PRESENT is 4 bit to 4 bit S-Box type. The LUT for the PRESENT algorithm is as given in table 2.

Table 2. LUT for PRESENT S-Box

P	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P (x)	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

For S-Box layer the current state $b_{63}.....b_0$ is considered as sixteen 4-bit words $W_{15}.....W_0$

Where for $0 \le i \le 15$, $W_i = b_{4*i+3} \| b_{4*i+2} \| b_{4*i+1} \| b_{4*i}$ for $0 \le i \le 63$[1].

On the pursuit of hardware efficiency, S-Box designed is 4 bit for being compact compared to 8-bit S-Box. To improve the avalanche effect of the S-Box designed with certain condition as follows [1]. Denoting the Fourier coefficient of S by

$$S_b^W(a) = \sum_{x \in F_2^4} (-1)^{(b,S(x))+(a,x)} \quad (4)$$

1. For any fixed non-zero input difference $\Delta_I \in F_2^4$ and any fixed non-zero output difference_ $\Delta_0 \in F_2^4$ we require

$$\#\{x \in F_2^4 \mid S(x) + S(x + \Delta_I) = \Delta_0\} \le 4 \quad (5)$$

2. For any fixed non-zero input difference $\Delta_I \in F_2^4$ and any fixed output difference $\Delta_0 \in F_2^4$ such that $wt(\Delta_I) = wt(\Delta_0) = 1$ we have

$$\{x \in F_2^4 \mid S(x) + S(x + \Delta_I) = \Delta_0\} \le 0 \quad (6)$$

3. For all non-zero $a \in F_2^4$ and all non-zero $b \in F_2^4$ it holds that $S_b^w(a) \le 8$.

4. For all $a \in F_2^4$ and all non-zero $b \in F_2^4$ such that wt(a) = wt(b) = 1 it holds that $S_b^w(a) = \pm 4$b.

B. The Modified Design of S-Box with RCA-30

The S-Box designed is 4 Bit to 4 Bit S Box with the modified logic within it. The Modification done in S-Box is based on application of Cellular Automata concept. Among the other rules of Cellular automata, Rule 30 was applied because of its reversibility function. The notation for the design follows as:

Here the preloaded constant value is denoted as ξ and input is denoted as 'x'

Input of the S- Box denoted as 'x'

$$A = S(i, \xi) \| S(i+1, \xi) \quad (7)$$

$$B = S(i-1, \xi) \sim (A) \quad (8)$$

$$y = S(i,x) \sim (B) \quad (9)$$

ξ ---> pre-loaded value --seed value or initialization vector

ξ +1 ---> output of S- Box

y ---> ξ +1

The output of the S-Box depends on the pre-loaded value since to get the randomness or wide transition loaded value to be given and checked. The randomness varied for each pre loaded value. In the figure 6, 'x' part is the input of S-Box and 'y' part is the output of S-Box. The transformation occurs in this part with the EX-OR operation shown in figure 6.

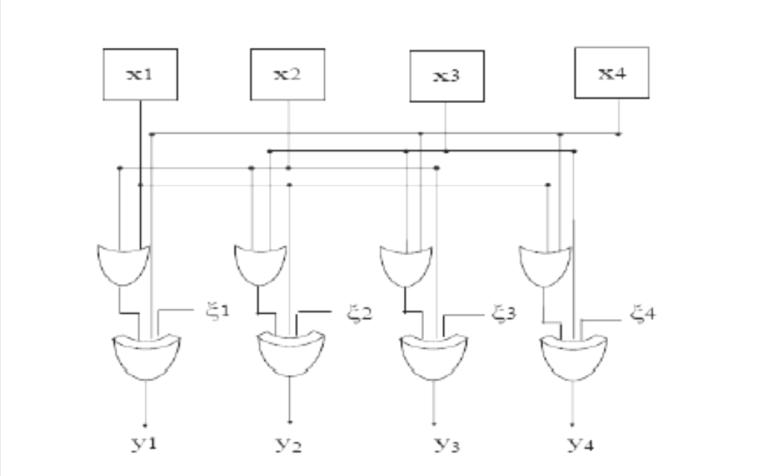

Fig. 6 Implementation Design RCA-30 [15].

C. AES S- Box Design

AES is the advanced encryption standard designed for the security for first time with LUT based as well as functionality based. The S-box design for AES is designed

based on LUT. The S-Box used here is 8 bit S-box. Since the PRESENT algorithm used LUT based S-box, here in AES also used the same. The possible variation in area and power will be obtained comparatively. 8-bit input to 8-bit affine output AES S-Box is shown in the figure 7. 8-bit sub byte transition by using composite field Arithmetic technique representation is shown in figure 7.

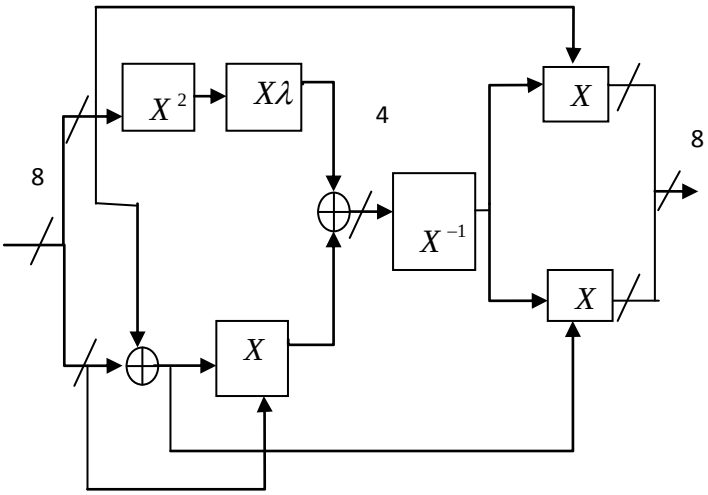

Fig. 7 Sub byte Using Composite Field Arithmetic Technique [16].

V. SYNTHESIZED RESULTS

The S-Box of PRESENT Encryption, RCA-30 and AES are analyzed for power, area and Security. The S- Box is designed to apply on encryption algorithm that would be PRESENT or AES. The modification is application of RCA - 30 on crypt process of PRESENT algorithm. The simulation results for S-boxes are shown and analysis report is given as follows. The implementation is done with Altera Cyclone III – EP2C5F256 and its analysis report is obtained from it.

The synthesis of three S-box are done and its analysis report is provide below. Here the Power is analyzed for Altera Cyclone III board EP2C5F256 at the frequency of 200MHz. At this frequency the power consumption by the device is mentioned. The same is analyzed with FPGA and reports for area and power are given.

Table 3.Comparison Table for various S-Box

S.NO	S-BOX	POWER at f 200MHz Cyclone III – EP2C5F256	AREA In terms of Logic consumed
1	PRESENT S-BOX	34.35mW	9
2	AES S-BOX	37.42mW	9
3	RCA-30 S-BOX	34.35mW	5

From the Table 3, Cyclone II device of Altera consume less power 34.35mW with RCA-30 S-Box. Hence the optimized power output and area is achieved with RCA-30 concept applied in S-Box.

VI. DISCUSSIONS

The analysis shows that power is reduced to certain extent in RCA-30 S-Box. Hence further reduction can be done by changing the functionality, since the reversibility is itself in the RCA logic the power consumption will be less. Comparing to AES, PRESENT occupies same area but more power. Using this RCA-30 S-Box with increasing complexity in the Key Schedule the security can be increased considerably. Since the minimal level of power is reduced in S-Box itself will lead to reduction of total power from the whole crypt process. Hence the attacks can be applied in the process to check the robustness of the it's security.

VII. CONCLUSIONS

The Power and area is analyzed for various S-Box such as PRESENT, AES and RCA-Rule 30. Here the Modified S-Box of PRESENT was reduced in power and area compared to PRESENT S-Box and report shown for 200MHz frequency. Hence with the reduced power of RCA Rule 30 S-Box, whole Crypt process can be done with low power and without compromise in Security level. So from the whole process the cryptanalysis can be done as future work to check the robustness of the security.

REFERENCES

[1] Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann,M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe ,"PRESENT: An Ultra-Lightweight Block Cipher", Springer Verlag 2007.

[2] Hoang Trang, Nguyen Van Loi, "An efficient FPGA implementation of the Advanced Encryption Standard algorithm", IEEE International Conference on Computing and Communication Technologies, Research, Innovation, and Vision for the Future (RIVF), pages 1-4, IEEE 2012.

[3] A.Biryukov, S.Mukhopadhyay, and P. Sarkar. Improved Time-memory Trade-offs with Multiple Data. In B. Preneel and S. Tavares, editors, Proceedings of SAC 2005, LNCS, volume 3897, pages 110-127, Springer Verlag 2005.

[4] Chi-Jeng Chang, Chi-Wu Huang, Hung-Yun Tai, Mao-Yuan Lin," 8-bit AES Implementation in FPGA by Multiplexing 32-bit AES Operation", First International Symposium on Data, Privacy and E-Commerce, IEEE 2007.

[5] Coppersnith D, Halevi S, Lutla C.S. "Cryptanalysis of stream cipher with linear masking." In: Yung M, eds. Advances in Cryptology-Crypto 2002. LNCS 2442, *Berlin: Springer-Verlag*, 2002. 515-532.

[6] Good.T, and Benaissa.M, "ASIC hardware performance," New Stream Cipher Designs: *The eSTREAM Finalists*, LNCS 4986, pp. 267–293, 2008.

[7] Jinyi Zhang, Qinghua Zuo , Tianbao Zhang, "Reducing the Power Consumption of the AES S-Box by SSC",IEEE 2007, 1-4244-1312-5.

[8] Lubos Gaspar, Milos Drutarovsky, Viktor Fischer, Nathalie Bochard," Efficient Aes S-Boxes Implementation For Non-Volatile FPGAs", IEEE 2009.

[9] Mohamed El-Hadedy, Danilo Gligoroski , Svein J. Knapskog and Einar Johan Aas "Low Area FPGA and ASIC Implementations of the Hash Function "Blue Midnight Wish-256", IEEE 2009.

[10] D.Mukhopadhyay and D. RoyChowdhury, "An Efficient End to End Design of Rijndael Cryptosystem in 0.18µm CMOS", Proceedings of the 18th International Conference on VLSI Design 2005.

[11] Rashmi Ramesh Rachh, P.V. AnandaMohan, B.S.Anami,"High Speed S-Box architecture for advanced encryption standard",IEEE 2011.

[12] Rose.G.G and Hawkes.G Turing "A Fast Stream Cipher" In Fast Software Encryption FSE 2003, pages 290-306. *Springer-Verlag*, 2003.

[13] Xinmiao Zhang and Keshab K. Parhi," An Efficient 21.56Gbps AES Implementation On FPGA", IEEE 2004.

[14] Yaobin Mao, Liu Cao and Wenbo liu,"Desing and FPGA Implementation of Psuedorandom bit Sequence Generator using Spatialtemopral Chaos",IEEE 2006.

[15] K.J.Jegadish Kumar, K.Chenna Kesava Reddy, S. Salivahanan, "Novel and Efficient Cellular Automata based Symmetric Key Encryption Algorithm for Wireless Sensor Networks", International Conference of Computer Application, PP 0975-8887, 2011.

[16] N.Anitha Christy and P.Karthigaikumar, "FPGA Implementation of AES Algorithm using Composite Field Arithmetic" ,2012 International Conference on Devices, Circuits and Systems, Pages 713 -717,IEEE 2012

