International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 23rd Jul 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-11&issue=Issue 07

DOI: 10.48047/IJIEMR/V11/ISSUE 07/13

Title **DESIGN OF EFFICIENT CRYPTOGRAPHY ARCHITECTURE USING GDI BASED MULTIPLIER**

Volume 11, ISSUE 07, Pages: 78-84

Paper Authors
BOLLEDDU SRUTHI, VENKATA RAO TIRUMALASETTY

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

DESIGN OF EFFICIENT CRYPTOGRAPHY ARCHITECTURE USING GDI BASED MULTIPLIER

[1]BOLLEDDU SRUTHI, [2]VENKATA RAO TIRUMALASETTY
[1]M.Tech Scholar, Dept of ECE, Malineni Lakshmaiah Womens Engineering College, Prathipadu Rd, Guntur, Andhra Pradesh, India
[2]Associate Professor, Dept of ECE, Malineni Lakshmaiah Womens Engineering College, Prathipadu Rd, Guntur, Andhra Pradesh, India

ABSTRACT: Due to privacy leakage of sensitive data, the conventional encryption systems are not completely secure from an intermediary service like cloud servers. The encryption mechanism has three security procedures, i.e., key generation, encryption and decryption. Modulo multiplier is one of the critical components in applications in the area of digital signal processing, data encryption and residue arithmetic that demand high-speed and low-power operation. Using GDI (Gate Diffusion Input) technique, implementation of a wide range of complex logic functions is possible using only two transistors. So, design of efficient cryptography architecture using GDI based Multiplier is presented in this project. Initially, input data bits and initial key is assigned to the preprocessing. Next, bits are substituted using S-Box. Here, Ultra low power and low area modulo multiplier is designed using the GDI technology is used which is the key operation of Cryptographic algorithm. After that shifting and mixing operation is performed. Now these bits are encrypted. Similarly, decryption process is reverse to this operation. Hence cryptography architecture based on GDI multiplier is implemented and it gives better security compared to exist one. The proposed design is implemented in Tanner EDA with 250nm technology. This system will provide better security, resource efficiency and high performance compared to existing CMOS technology based design.

KEYWORDS: Cryptography, encryption, Decryption, GDI (Gate Diffusion Input), S-Box, Modulo Multiplier, Tanner EDA tools.

I. INTRODUCTION

Cryptography is the process adopted to ensure the secure storage of data in an unprotected storage place by avoiding the eaves drops [1]. Confidential data exchange over public computer network is achieved by authentication, confidentiality and integrity. Cryptography is the process adopted to ensure the secure storage of data in an unprotected storage place by avoiding the eaves drops. The cryptography technique converts plain text into cipher text using some key which is not readable format others then it transmitted through channel again cipher text is converted into plain text at receiver end using key [2]. The encryption and decryption of encryption algorithms are performed by repeated modulo multiplications. These multiplications differ from those encountered in signal processing and general computing applications in their sheer operand size. key sizes are typically very high, hence the key multiplication becomes very difficult and the long carry propagation of large integer multiplication is limited the entire system performance [3].

CMOS multipliers occupy substantial area and power in digital circuits. To further optimize power and area, it is required to reduce the number of devices in design of multipliers. This can be implemented using a revised CMOS logic viz., GDI technique. Circuits designed in GDI are based on GDI basic cell which allows us to apply more than one input (G,P&N) to a device unlike in CMOS circuits [4]. GDI is a new technique of low-power digital combinational circuit design. This technique allows reducing power consumption, propagation delay, and area of digital circuits while maintaining low

complexity of logic design. Pass-transistor logic has been presented for NMOS. They are based on the model, where a set of control signals is applied to the gates of NMOS transistors. However, most of the PTL implementations have two basic problems. They are since the "high input voltage level at the regenerative inverters is not VDD, the PMOS device in the inverter is not fully turned off, and hence Direct-path static power dissipation could be significant. A new low-power design technique that allows solving most of the problems mentioned above called GDI technique. The GDI approach allows implementation of a wide range of complex logic functions using only two transistors. This method is suitable for design of fast, low-power circuits, using a reduced number of transistors (as compared to GDI and existing PTL techniques), while improving logic level swing and static power characteristics and allowing simple top-down design by using small cell library. So in this paper efficient cryptography architecture using GDI based multiplier is design and implemented using Tanner EDA tool.

II. LITERATURE SURVEY

In [5] Hossein Mahdizadeh and Massoud Masoumi presented a Novel architecture for efficient FPGA implementation of elliptic curve cryptographic processor over GF(2'63).In that implementation the execution delay of the LD algorithm was reduced by parallelization of the multipliers. The hardware implementation of the elliptic curve cryptographic processor was designed with the objective of area reduction. Shoaleh Hashemi Namin et al in [6] elaborated the Power Efficiency of Digit Level Polynomial Basis Finite Field Multipliers in GF(2283). The brief reported area utilization of 15776l.2 critical delay of 5.46ns and an energy delay product of 2036.4. S. Farah, M. Y. Javed, A. Shamim, and T. Nawaz in [7]. This paper presents the evaluation of RSA, ElGamal & Pallier asymmetric encryption algorithms. Encryption algorithms provide a secure communication over the internet and play main role in any security system. These algorithms consume a considerable amount of time and resources such as memory, CPU time, battery power and computation time to encrypt and decrypt data. In this paper, different experiments have been conducted to compare these algorithms in term of encryption time, decryption time, memory usage and throughput over variable text file and private key sizes

In 2011 however, four years before the announcement of the NSA, Jao and Feo [8] published a paper proposing a different approach for Elliptic Curve Cryptography systems which would be resistant quantum attacks based on Shor's algorithm. A. Al Hasib and A. A. M. M. Haque in [9], Security is always a major concern in the field of communication. Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) algorithms are the two popular encryption schemes that guarantee confidentiality and authenticity over an insecure communication channel. There has been trifling cryptanalytic progress against these two algorithms since their advent. This paper presents the fundamental mathematics behind the AES and RSA algorithm along with a brief description of some cryptographic primitives that are commonly used in the field of communication security. It also includes several computational issues as well as the analysis of AES and RSA security aspects against different kinds of attacks including the countermeasures against these attacks.

Kenney, R. D., *et.al*., [10], have provided a motivation to implement decimal arithmetic in hardware. They have presented a repetitive decimal multiplier.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

This decimal multiplier works at relatively higher frequencies of clock. This type of multiplier is suitable for the designs if the size of the operands is large. This multiplier makes use of a freshly new representation for the intermediate products. This decimal representation is allowed for a very high speed 2-stage multiplier design. An overloaded decimal representation is used to store the intermediate products. This representation allows the use of BCD digits which invalid. Decimal multipliers are implemented in Verilog language for a number of different digit operands. The result of synthesis shows that the circuits work with the approximate frequency of clock as 2 GHz if it is designed by making use of a 0.11 micron CMOS standard cell library.

III. PROPOSED DESIGN

The proposed algorithm performing operations on input data i.e. plain text and utilizes identical key for both encryption & decryption. Thee below figure (1) representing the architecture of secure GDI multiplier based cryptography architecture.

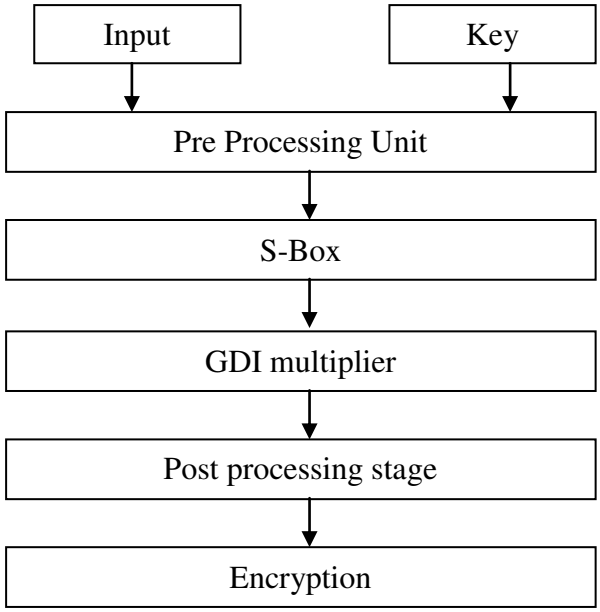

Fig. 1: PROPOSED EFFICIENT CRYPTOGRAPHY ARCHITECTURE USING GDI BASED MULTIPLIER

In each cipher round, preprocessing, S-Box, GDI multiplier, Post processing and encryption are performed. The plaintext is Exclusive-ORed with initial key of in initial round at preprocessing stage. This algorithm operates on compromised data block of 4 x 4 byte matrix called as state. Proposed algorithm essential procedures are carried on the state. While for high speed applications GDI based multiplier architecture is generally utilized for modular multiplication stage in cryptography architecture. ShiftRows() and MixColumns() transformations are performed on a two dimensional 4×4 array of bytes known as states in the post processing stage and finally encrypted output called cipher is generated at encryption output. Decryption is also perfumed in the same way of encryption but in reverse process using inverse S-box and inverse GDI multiplier blocks.

3.1 Preprocessing

It computation a pair of signals in this phase namely generate and propagate signals, which corresponds to each ith state of A and B input sets. Propagate and generate signal are represent as shown below Based on initial key, keys are generated for algorithm in each cipher round. Bitwise XOR operation is performed by Roundconst function utilizing round constant array.

3.2 S-Box

The values of S – box are calculated in the finite field GF(2^n) by taking multiplicative inverse, where the input with all zero bits is mapped itself & applying affine transmission on GF(2^n). In the finite field GF(2^n) multiplicative inverse is given in Eq.(1).

$$S(y) = Affine\ transform\ (y^{-1}) \quad \text{---- (1)}$$

S-box values generation using PN Sequence Generator: For generating sequence of pseudorandom binary numbers

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

A PN Sequence Generator is utilized. A LFSR (Linear Feedback Shift Register) which is described by generator polynomial is used for designing a PN sequence generator. LFSR is a shift register and its input bit is a previous state linear function which is generated by XORing selected bits from all bits of shift register. Generator polynomial feedback taps determined the number of stated generated by LFSR. The AES algorithm S – box contains 2^n distinct n bit values. The S – box values generation, PN sequence generator is utilized with feedbacks tap maximal length for generating $2^n - 1$ random values across $(01)_h$ to $(FF)_h$. The value $(00)_h$ is fed randomly in to the S – box. For generating maximum length sequence of 8-bit, The polynomial generator will be set to any of the following feedback taps viz.

The bits are XORed & feedback from MSB over each clock cycle results in previous value cycle shifting. By giving a feedback to generator input and combining shift register feedback tap elements to obtain random sequence with a very large reception period. The output values randomness generated from PN sequence generator not only depends on feedback taps but also depends on non – zero initial n – bit seed value applied to the generator. The changes in seed value changes the generated sequence values and shifts the initial value, which can resulting as generating sequence only known to the designers. These values can be used for S – box formation. For strengthening the AES algorithm against different attacks the invertible S- box is responsible. The lack of knowledge on the feedback taps & selected seed value to the attackers can make AES algorithm invulnerable to attacks. The state matrix individual bytes are replaced by corresponding value which is stored in S- box modified in SubBytes transformation. For this the lower nibble & higher nibble of state matrix individual entry is considered as column & row of S –box respectively.

3.3 GDI Multiplier

The efficient design of cryptographic algorithms presented in this paper used for secured transmission of data. There three major components that's decide the overall power area and performance of this. They are modulo 2^n addition, bitwise-xor and modulo 2^n+1 multiplier. Modulo 2^n addition and bitwise-xor will take less time and easy to implement improving the area and power efficiency of modulo 2^n+1 multiplication operation leads to significant decrease in area and power consumption of the encryption cipher. Therefore introducing new low power design technique called GDI (Gate-Diffusion-Input) technology Instead of CMOS technology. Modulo multiplier have three major blocks partial product generation, partial product reduction, and final stage addition. The partial product reduction block use the GDI EXOR gates this area of the partial product block which will reduced to 65% of the area. In the partial product generation blocks we will use GDI based AND and OR gates.

From the n × n partial product matrix, it is possible to observe that the partial product generation requires AND, OR and NOT gates. The most complex function of partial product generation module is $p_{n-1,n-1}V_{q_{n-2}}$ where $P_{i,j} = a_1 b_j$ and $q_1 = P_{n,1}VP_{1,n}$. The partial product reduction unit is the most important module which mainly determines the critical path delay and the overall performance of the multiplier. Hence this module needs to be designed so as to get minimum area and consume less power. In the partial products reduction module, the n×n partial product matrix and the constant 3(i.e., correction factor) need to be added to produce the final sum and carry vectors.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

The n partial products should be added to produce the final n-bit Sum and Carry vectors. In a single stage of the Carry Save Addition, series of n full adders take 3 input operands and produce two n-bit output vectors. To add n+1 input operands, n-1 Carry Save Addition stages are required in the partial products reduction module. As the first partial product is the constant 2, in the first stage of the n-1 CSA stages, half adders can be used instead of full adders except for the for the second bit. The n-1 stage CSA can be implemented using n full adders in each column of the n-1 stages. In this regular implementation, series of full adders in the CSA adder columns can be replaced by the proposed GDI EXOR-based compressors that take the same number of inputs, which leads less power implementation of the multiplier.

4.5 Post Processing Stage

In this post processing stage shiftrows transformation and MixColumn Transformations are performed. In ShiftRows transformation the state matrix shift rows are cyclically shifted towards the left by respective positions. The offset value is depends on row number. Thus 1st row remains unchanged. Rows cyclic rotation imparts a diffusion property in AES algorithm. The transformation of MixColumns performs operations on the each column of state matrix one at a time. This transformation is linear diffusion process. In state matrix each column is taken as a n/2 – term over GF(2^n). The column is then multiplied by modulo ($y^{n/2}$+1) with a fixed polynomial a(y) given by Eq. (3),

$$a(y) = \{03\}y^3 + \{01\}y^2 + \{01\}y^1 + \{02\} \quad \text{---- (2)}$$

Eq.(3) can also be represented as matrix multiplication as Eq. (4):

$$p'(y) = a(y) \times p(y) \text{---- (3)}$$

and in matrix form as Eq. (5):

$$\begin{bmatrix} P'_{0,c} \\ P'_{1,c} \\ P'_{2,c} \\ P'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 00 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} P_{0,c} \\ P_{1,c} \\ P_{2,c} \\ P_{3,c} \end{bmatrix} \text{---- (4)}$$

4.6 Encryption

A homomorphic encryption is an scheme of augmented encryption scheme is used which is having two additional routines HE.Mult() & HE.Add() for performing add or multiply on encrypted data. Because of mathematical homomorphism, the result is still a ciphertext (encrypted data) encrypting the sum of plain texts or respectively the of t plaintexts products. In a untrusted cloud the users may upload their ciphertext and still computations can be performed on ciphertext without the requirement of decryption. The existing HE schemes are having noisy in nature. During encryption noise is used for message hiding. Noise increases in the resulting cipher text due to each homomorphic evaluation on cipher text. If noise threshold is beyond then further more homomorphic evaluations results in decryption failures. This threshold value calls hamomorphic scheme depth and it is found out by parameter choice set (e.g coefficients size & data structures length, etc.). In a simple view hammomorphic encryption scheme depth is analogous to circuit 'critical path'.

IV. RESULTS

Supply voltage of 5v with 220nm technology of Tanner EDA tool is used in the simulation results. Based on same input patterns the circuit has to be tested in order to create an independent environment for testing. The designing of 4-bit Cryptography architecture using GDI based multiplier can be achieved. Proposed GDI logic consumption power and transistors used count are compared with the pass transistor Complementary logic. Modulo multiplier is designed on the basis

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

of GDI. The following figure (6.1) shows the schematic of proposed efficient Cryptography architecture using GDI based multiplier.

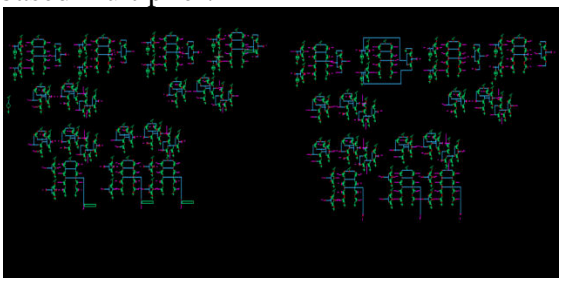

Fig. 2: CIRCUIT SCHEMATIC OF PROPOSED SYSTEM

Here, A0, A1, A2, A3 are the input data to be encrypted and B0, B1, B2, B3 are four bit initial key applied at the input stage of encryption unit. Then the encrypted outputs are p0, S1, S2, and S3.

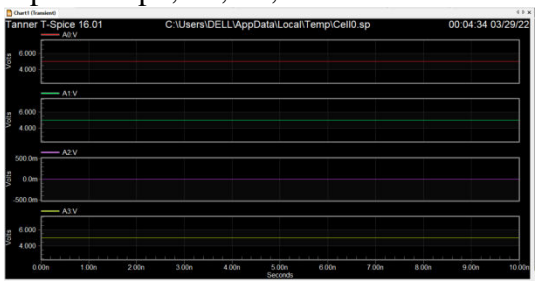

Fig. 3: WAVEFORMS OF INPUT BITS

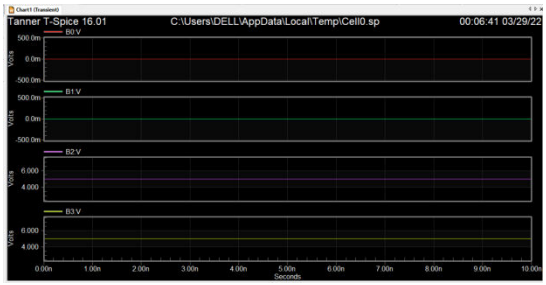

Fig. 4: WAVEFORMS OF INITIAL KEY

The A0=1, A1=1, A2=0, A3=1 and B0 =0, B1=0, B2=1, B3=1 are the given databits and p0=1, S1=1, S2=1, S3=0 are the encrypted outputs.

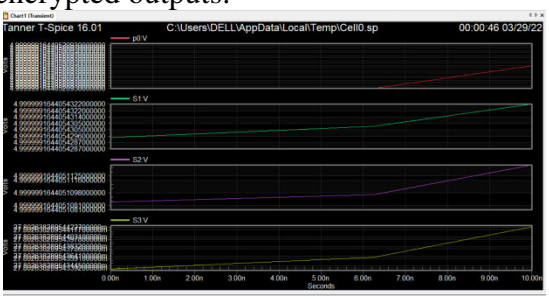

Fig. 5: OUTPUT WAVEFORMS OF ENCRYPTION

The decryption output are considered as pp0, SS1, SS2, SS3 and are obtained as pp0=1, SS1=1, SS2=0, SS3=1

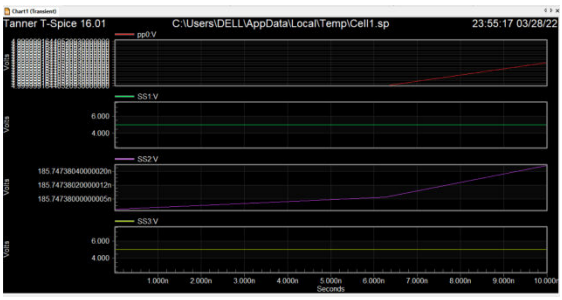

Fig. 6: OUTPUT WAVEFORMS OF DECRYPTION

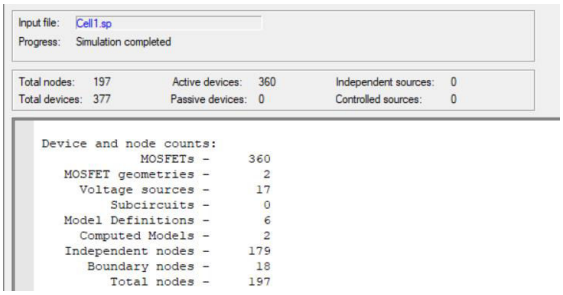

Fig. 7: SIMULATION RESULT OF PROPOSED DESIGN

The result of GDI is having less number of transistor utilization thereby area to implement the design is also reduced. The number of boundary nodes and independent node as shown in figure (7) are also less that leads to low critical path delay lead to high speed of operation.

V. CONCLUSION

In this project, design of efficient cryptography architecture using GDI based multiplier was implemented. First, the S-box values are generated by the PN Sequence Generator. Based on PN Sequence Generator the required initial key for encryption/decryption is generated. Then private key & public key can shifts the bits in one clock cycle. An efficient polynomial – basis inversion and multiplication was developed using an area efficient GDI (Gate diffusion input) based multiplier as module multiplier in this document. The cryptography architecture was designed and implemented in Tanner

EDA tools and this system provides security in efficient way & it is faster. The simulation shows that the design is more efficient with less surface area and is faster. It achieved due to decrease in transistor counts than CMOS. Based on the overall performance analysis it can be concluded that this design provides better performance than others in terms of the area and the timing.

VI. REFERENCES

[1] Rajat Sadhukhan, Debdeep Mukhopadhyay, "Design Automation for Side Channel Resistant Lightweight Cryptography", 2020 IFIP/IEEE 28th International Conference on Very Large Scale Integration (VLSI-SOC), 2020

[2] Alshaima Q. Al-Khafaji, M. F. Al-Gailani, Hikmat N. Abdullah, "FPGA Design and Implementation of an AES Algorithm based on Iterative Looping Architecture", 2019 IEEE 9th International Conference on Consumer Electronics (ICCE-Berlin), 2019

[3] Veronica Ernita Kristianti, Eri Prasetyo Wibowo, Atit Pertiwi, Hamzah Afandi, Busono Soerowirdjo, "Finding an Efficient FPGA Implementation of the DES Algorithm to Support the", 2018 2nd East Indonesia Conference on Computer and Information Technology (EIConCIT), 2018.

[4] Prashanthi Metku, Kyung Ki Kim, Yong-Bin Kim, Minsu Choi, "Low-Power Null Convention Logic Multiplier Design Based On Gate Diffusion Input Technique", 2018 International SoC Design Conference (ISOCC), 2018

[5] Hossein Mahdizadeh and Massoud Masoumi, ""Novel architecture for efficient FPGA implementation of elliptic curve cryptographic processor over GF(2'63)", IEEE Transactions on very large scale integration (vIs i) systems, Vol. 21, No. 12, pp: 2330- 2333, Dec.2013

[6] Shoaleh Hashemi Namin, Huapeng Wu, Majid Ahmadi, "Power Efficiency of Digit Level Polynomial Basis Finite Field Multipliers in GF(2283)", International conference on electronics, circuits and system, pp: 897-900, Dec.2012

[7] S. Farah, M. Y. Javed, A. Shamim, and T.Nawaz, "An experimental study on Performance Evaluation of Asymmetric Encryption Algorithms,"Recent advaces Inf. Sci., vol. 8, pp. 121– 124, 2012.

[8] D. Jao, and L. Feo, Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies, in Post-Quantum Cryptography Lecture Notes in Computer Sciences, pp. 19-34, 2011.

[9] A. Al Hasib and A. A. M. M. Haque, "A comparative study of the performance and security issues of AES and RSA cryptography," Proc. - 3rd Int. Conf. Converg. Hybrid Inf. Technol. ICCIT 2008, vol. 2, no. November 2001, pp. 505–510, 2008.

[10] Kenney R. D., Schulte M. J., and Erle M. A., "A high-frequency decimal multiplier," *IEEE International Conference on computer Design*: VLSI in Computers and Processors (ICCD), pp. 26-29, October 2004

[1]**BOLLEDDU SRUTHI** completed B.Tech from Bapatla Women's Engineering College, Karlapalem, Bapatla, ANdhrapradesh, India and doing m.tech with VLSI Design specialization at Malineni Lakshmaiah Womens Engineering College, Prathipadu Rd, Guntur, Andhra Pradesh, India.

[2]**VENKATA RAO TIRUMALASETTY** completed B.Tech from Malineni Lakshmaia Engineering college, Guntur, Andhra Pradesh, India and M.Tech from Vignan's Foundation for Science, Technology & Research (Deemed to be University), Vadlamudi, Guntur, Andhra Pradesh, India. He has 10 years of teaching experience and working as Assistant professor at Malineni Lakshmaiah Womens Engineering College, Prathipadu Rd, Guntur, Andhra Pradesh, India. He has professional membership in IAENG. His interested area of research is Low Power VLSI Design.