International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 3, Issue 7, July 2014

DETECTION OF SECURITY ATTACKS BY USING TEST PATTERN GENERATION METHOD

(CHAITANYA SAI L)[1] (R KALYAN)[2] (V KEERTHY RAI)[3]
[1](STUDENT, DEPT OF ELECTRONICS AND COMMUNICATION ENGINEERING, SWETHA INSTITUTE OF TECHNOLOGY AND SCIENCE, TIRUPATI, INDIA)
[2](ASSISTANT PROFESSOR, DEPT OF ELECTRONICS AND COMMUNICATION ENGINEERING, SWETHA INSTITUTE OF TECHNOLOGY AND SCIENCE, TIRUPATI, INDIA)
[3](HOD, ASSISTANT PROFESSOR ,DEPT OF ELECTRONICS AND COMMUNICATION ENGINEERING, SWETHA INSTITUTE OF TECHNOLOGY AND SCIENCE, TIRUPATI, INDIA)

Abstract—Hardware implementation of cryptographic algorithms is subject to various attacks. It has been previously demonstrated that scan chains introduced for hardware testability open a back door to potential attacks. Here, we propose a scan-protection scheme that provides testing facilities both at production time and over the course of the circuit's life. The underlying principles to scan-in both input vectors and expected responses and to compare expected and actual responses within the circuit. Compared to regular scan tests, this technique has no impact on the quality of the test or the model-based fault diagnosis. It entails negligible area overhead and avoids the use of an authentication test mechanism.

1.Introduction:

Cryptography is the science of secure communication and information protection from unauthorized access. Cryptography enables communicating parties to exchange information securely over an insecure channel. Modern cryptography not only applies to secure communication, but also has applications in software security, security of electronic devices (smart cards, RFIDs, memories, etc.), data protection (disk encryption), copyright protection (Digital Rights Management (DRM)) and more. Examples include RFID based access control systems, authenticating users for bank transactions using smart cards supporting cryptographic protocols, and full hard disk encryption employing symmetric-key cryptography. Cryptography as a technology can be used to provide the following security properties: confidentiality of data, data integrity,

Entity authentication of the sender and the receiver, and non-repudiation of sender and receiver, among others [89]. Various cryptographic primitives and protocols can help in attaining these objectives. Though the mathematical or theoretical strength of these primitives can be quite high, their implementations in hardware or software are prone to information leakages. Cryptographic implementations in hardware and software need to be protected against attacks aimed at revealing the secret information stored within them. Hardware attacks can be characterized as follows:

- Active or passive attacks: active attacks require the attacker to tamper or perturbate the device internals (by probing, laser impingement, etc.) and derive the secret data from the observed response. Passive attacks require the attacker to only observe passively and infer the secret from the observed behavior by exploiting one or more physical characteristics of the device when it is in operation. Some of these characteristics include power consumption, electromagnetic radiation, execution timing, or the data coming in or out of the external interface.
- Invasive, semi-invasive or non-invasive attacks: invasive attacks require opening the device package and contact the electronic circuits inside; semi invasive attacks also require opening the device package but no contact to the internal circuits is needed, while non-invasive attacks do not require modification of the device package.

The non-invasive and passive attacks are also termed as side-channel attacks where the physical characteristic opens a side-channel or backdoor

 All Rights Reserved © 2014 IJARECE

through which secret information inside the cryptographic chips leaks. Some of these side-channels include electromagnetic radiation or power consumption of the circuit in operation. In this thesis, we focus on one such side-channel which is the Design-for-Test (DfT)

Infrastructure incorporated in a circuit for thorough and rapid manufacturing test of the device. Scan chains are widely deployed in the semiconductor industry for structural testing after manufacturing or fabrication. Although scan chain DfT provides the highest testability, it can be used by an attacker to read chip-internal data, read stored secret information and determine the positions of all the secret elements in a chain. Scan chains may be permanently disabled after testing of the chip (by blowing some fuses, for instance) before being used in a product, but then the in-field testability of the chip is lost. Probing attacks can still be performed on parts of these broken scan chain elements and even the blown fuses can be carefully connected back. Moreover, the area cost to incorporate these fuses can be quite high.

Hence, in this thesis, scan chains have been left intact for thorough testing of complex circuits, but at the same time protected against attacks exploiting the test infrastructure. The mechanism to achieve this dual paradigm of test and security should not add high area overhead or increase the test time to an unacceptable level. Hence, the purpose of this thesis is to design secure DfT structures which address the trade-off between security, test quality and test cost.

This brief is organized as follows. Section II summarizes the most relevant design-for-testability-and-security proposals from the literature, and discusses their related drawbacks. The detailed implementation of the module in charge of the proposed test strategy is described in Section III, and related costs and impact in terms of insertion in the design flow are also presented. Section IV discusses security, testability, and diagnostic issues related to the introduction of the proposed test scheme. Finally, Section V concludes on this brief.

Scan has been generally accepted as the standard method of testing chips due to high fault coverage and relatively lower area overhead. Inserting scan-chains while designing the chip requires a few additional/multiplexed pins to the primary inputs/outputs to serve as the scan-enable, scan-inputs and scan-outputs. Internally, there is little impact on the design since the standard flip-flops (FFs) are replaced by scan flip-flops (SFFs) (i.e., flip-flops with an input multiplexer) which are then linked to one another creating a shift register (scan chain). An example of a scan chain is shown in the Figure 1.1. Scan-enable selects between functional and test mode operations. It controls each multiplexer, choosing between the normal mode input of the FF or the output of the previous SFF in the chain.

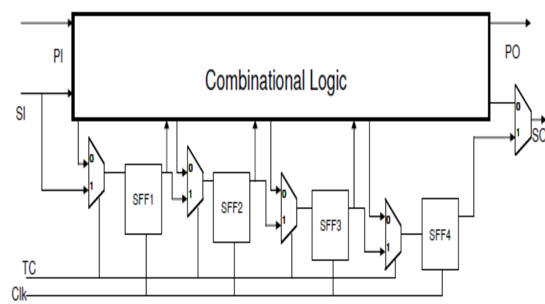

Figure 1.1: Scan chain DfT structure

II SECURITY, TEST, AND DIAGNOSTIC ISSUES

This section discusses the security improvements related to the observation of a single pass/fail result as well as issues related to test and diagnosis.

A. Security Analysis

The role of the proposed Secure Comparator is to avoid the observation of SFFs containing secret information. If the result of

 All Rights Reserved © 2014 IJARECE

the comparison was accessible at each clock cycle instead of each test vector, an attacker could easily observe the scan chain content by shifting in "000…000" on the *S*exp pin. Each bit-comparison would then validate that either the actual bit was "0" when TestRes = 1 and vice versa. On the contrary, with the proposed vector-wise comparison, the only way to retrieve the sensitive data information is to apply a brute-force attack by trying every possible response until TestRes is asserted. This attack would thus require 2#SFF attempts. If other attacks such as side-channel attacks [16] or faults attacks [17] are dreaded, the Secure Comparator has to be protected as the rest of the circuit. Even if countermeasures can lead to a large area overhead (e.g., [18]) their implementation concerns a very small part of the circuit.

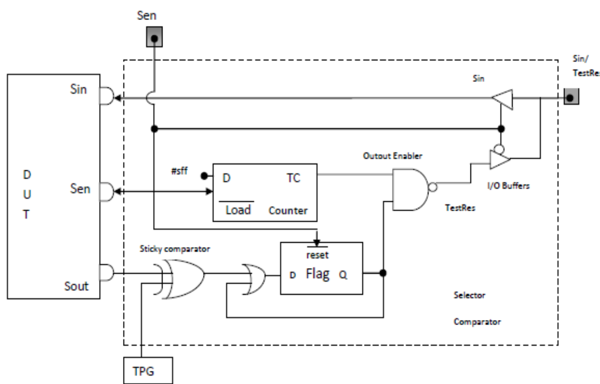

Fig 2.1 Proposed Secure comparator Using Test Pattern Generator

B. Testability

The secure comparator does not impact the fault coverage. In fact, each test response is compared to the expected one as in a classical ATE-based test scheme. Therefore, the achievable fault coverage is not altered. Test time is not increased either, since the expected responses are scanned-in at the same time as the next input vector is scanned-in. Concerning the test of the Secure Comparator itself, any DfT technique controlled by the external ATE (e.g., a dedicated scan chain to test the counter of the Output Enabler) would jeopardize the overall security. Nevertheless, the Secure Comparator can be totally tested by using only its inputs (*S*en, *S*exp, *S*in, and TestRes).

We have identified a procedure to test all stuck-at faults no matter of the size of the Secure Comparator. This functional test involves the comparison of the actual SFF values with a partially matching, a fully unmatching, and a correct response. Moreover, it includes the application of a two unmatching responses without the intermediate capture cycle, and twice the execution of the capture cycle. This test procedure requires 6· (#SFF+1) clock cycles to provide 100% stuck at fault coverage.

A limitation of our technique is related to the presence of possible unpredictable values in the SFFs. Computing expected values for the on-chip comparison is indeed no longer possible. To fix this limitation, the Sticky Comparator should ignore the comparison result (and keep unchanged its flag) when *S*out is unknown. This can be implemented by providing an additional mask signal that is asserted when needed. However, an attacker must not be able to mask as many bits as wanted.

In fact, if it were possible to mask all but one bit, it would be obvious to discover the value of each single bit in the scan response. This would reduce the complexity of the brute-force attack from exponential [O(2#SFF*)*] to linear [O(#SFF)]. The extra cost to tolerate unknown values includes an extra pin for the mask, a log2 P counter to limit the number of masked bits and two logic gates. Fig. 2 shows a possible implementation.

III Results

3.1 Secure Comparator

 All Rights Reserved © 2014 IJARECE

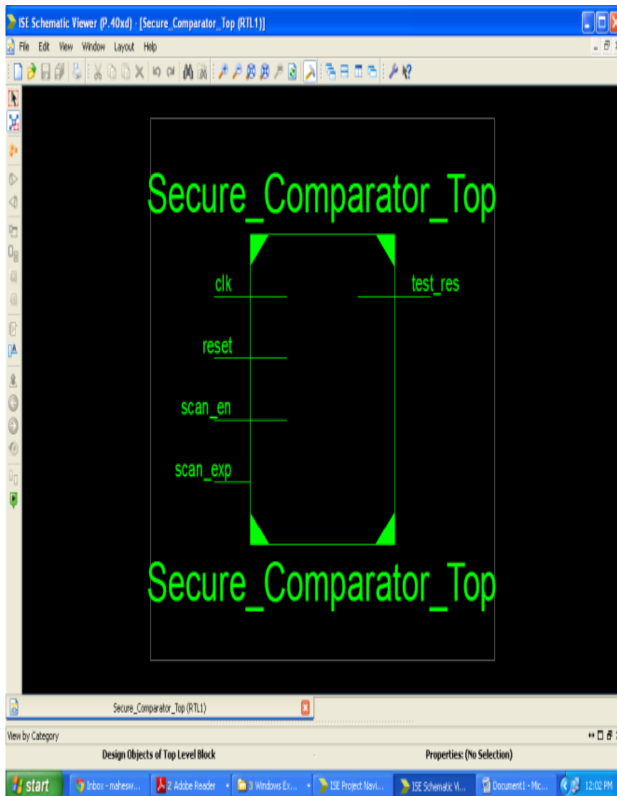

Fig 3: RTL Schematic Secure Comparator

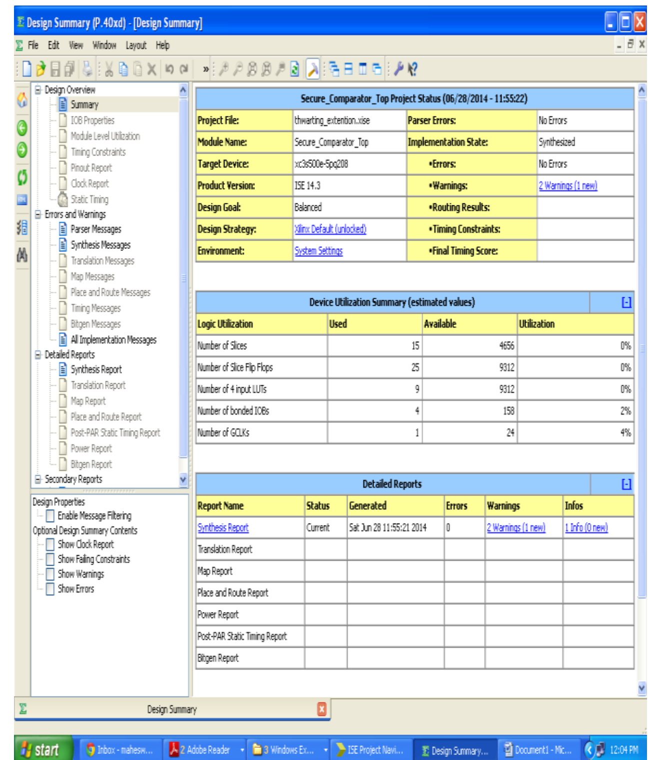

Fig5: Design Summary

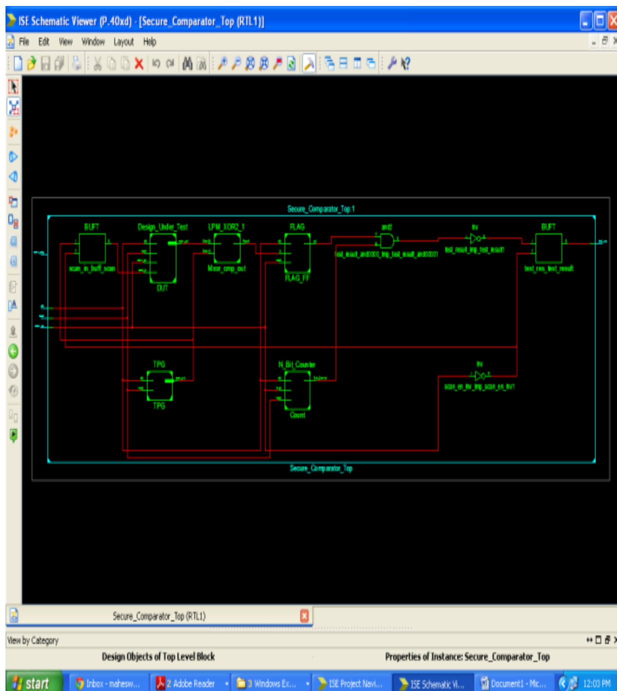

Fig4: Technology Schematic of Secure Comparator

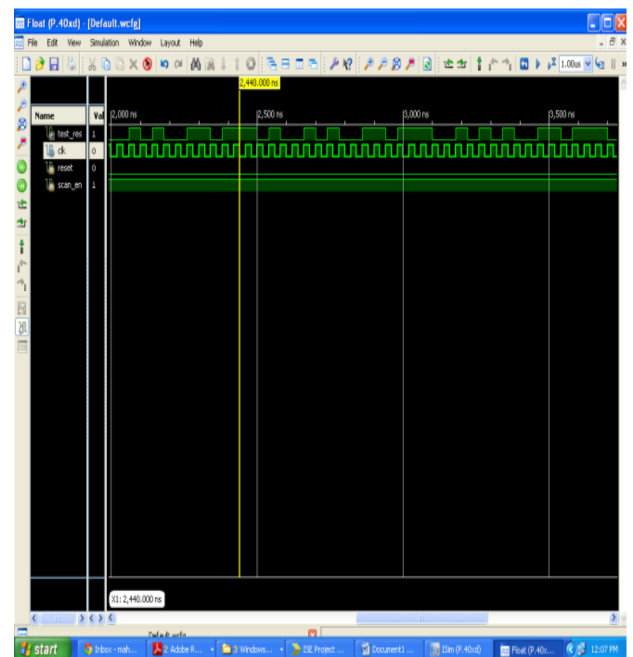

Fig 6: Simulation Results

 All Rights Reserved © 2014 IJARECE

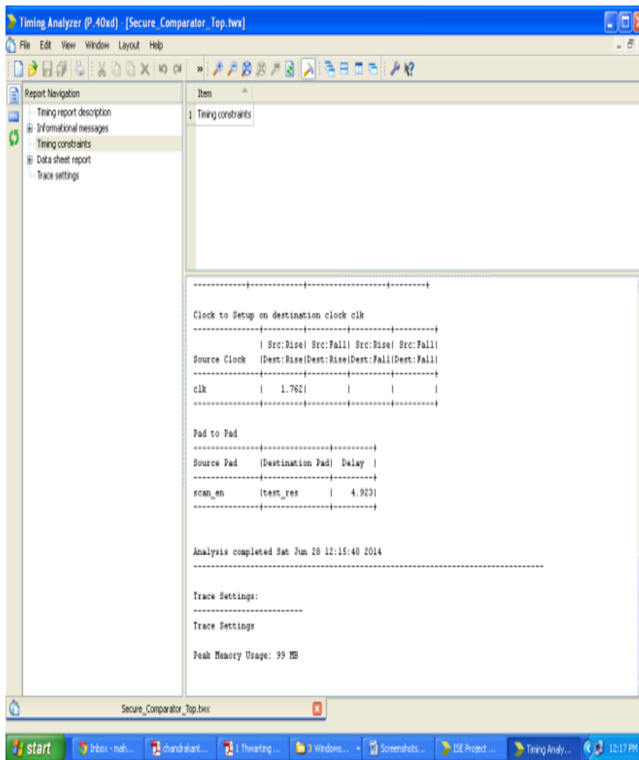

Fig7: Delay Report

3.2 Test Pattern Generator

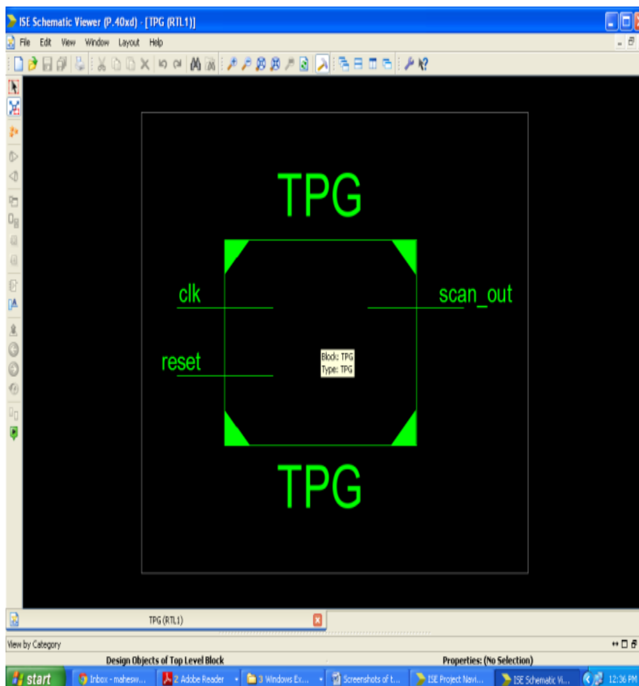

Fig8: RTL Schematic of Test Pattern Generator

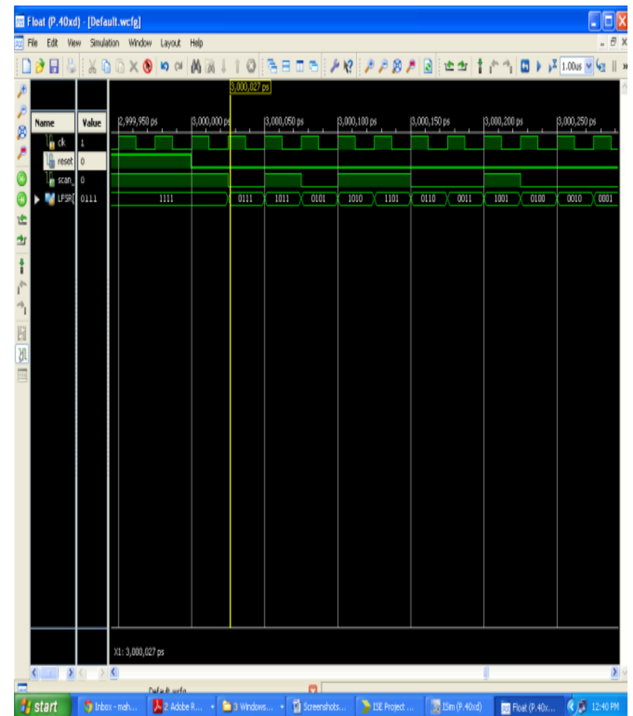

Fig 9 :Simulation Results

V.REFERENCES

[1] B. Yang, K. Wu, and R. Karri, "Secure scan: A design-for-test architecture for crypto chips," *IEEE Trans. Computer.-Aided Design Integr.Circuits Syst.*, vol. 25, no. 10, pp. 2287–2293, Oct. 2006.

[2] B. Yang, K. Wu, and R. Karri, "Scan based side channel attack on dedicated hardware implementations of data encryption standard," in *Proc. IEEE Int. Test Conf.*, Oct. 2004, pp. 339–344.

[3] Y. Wu and P. MacDonald, "Testing ASICs with multiple identical cores,"*IEEE Trans. Computer.-Aided Design Integr. Circuits Syst.*, vol. 22, no. 3,pp. 327–336, Mar. 2003.

[4] K. J. Balakrishnan, G. Giles, and J. Wing field, "Test access mechanism in the quad-core AMD opteron microprocessor," *IEEE Design TestComput.*, vol. 26, no. 1, pp. 52–59, Jan. 2009.

[5] D. Andreu, "System and method for wirelessly testing integrated circuits,"U.S. Patent 0 244 814, Oct. 6, 2011.

[6] F. Poehl, M. Beck, R. Arnold, J. Rzeha, T. Rabenalt, and M. Goessel,"On-chip evaluation, compensation and storage of scan diagnosis

 All Rights Reserved © 2014 IJARECE

data,"*IET Comput. Digit. Tech.*, vol. 1, no. 3, pp. 207–212, 2007.

[7] G.-M. Chiu and J. C.-M. Li, "A secure test wrapper design against internal and boundary scan attacks for embedded cores," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 20, no. 1, pp. 126–134,Jan. 2012.

[8] K. Rosenfeld and R. Karri, "Attacks and defenses for JTAG," *IEEE Design Test Comput.*, vol. 27, no. 1, pp. 36–47, Jan. 2010.

[9] C. J. Clark, "Anti-tamper JTAG TAP design enables DRM to JTAG registers and P1687 on-chip instruments," in *Proc. IEEE Int. Symp. Hardw.-Oriented Security Trust*, Jun. 2010, pp. 19–24.

[10] D. Hely, F. Bancel, N. Berard, M. L. Flottes, and B. Rouzeyre, "Test control for secure scan designs," in *Proc. IEEE Eur. Test Symp.*,May 2005, pp. 190–195.

[11] D. Hely, M.-L. Flottes, F. Bancel, B. Rouzeyre, N. Berard, and M. Renovell,"Scan design and secure chip [secure IC testing]," in *Proc. IEEEInt. On-Line Test. Symp.*, Jul. 2004, pp. 219–224.

[12] G. Sengar, D. Mukhopadhyay, and D. R. Chowdhury, "Secured flipped scan-chain model for crypto-architecture," *IEEE Trans. Comput.-AidedDesign Integr. Circuits Syst.*, vol. 26, no. 11, pp. 2080–2084, Nov. 2007.

[13] H. Fujiwara and M. E. J. Obien, "Secure and testable scan design using extended de Bruijn graphs," in *Proc. Asia South Pacific Design Autom.Conf.*, 2010, pp. 413–418.

[14] J. Da Rolt, G. Di Natale, M.-L. Flottes, and B. Rouzeyre, "New securitythreats against chips containing scan chain structures," in *Proc. IEEE Int.Symp. Hardw.-Oriented Security Trust*, Jun. 2011, pp. 110–115.

[15] L. Chunsheng and Y. Huang, "Effects of embedded decompression and compaction architectures on side-channel attack resistance," in *Proc.IEEE VLSI Test Symp.*, May 2007, pp. 461–468.

[16] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc.Int. Cryptol. Conf. Adv. Cryptol.*, 1999, pp. 388–397.

[17] P. Dusart, G. Letourneux, and O. Vivolo, "Differential fault analysis on A.E.S," in *Applied Cryptography and Network Security*, vol. 2846. NewYork, NY, USA: Springer-Verlag, 2003, pp. 293–306.

[18] A. Moradi, T. Eisenbarth, A. Poschmann, C. Rolfes, C. Paar, M. T. M.Shalmani, and M. Salmasizadeh, "Information leakage of flip-flops in DPA-resistant logic styles," in *Proc. IACR Cryptology ePrint Archive*,2008, pp. 188–188.

Authors:

Miss. L Chaitanya Sai received the B.Tech (ECE) from SWETHA institute of Technology and science, Tirupati, India, JNTU Anantapur, India, in 2012 and pursuing M.Tech (VLSI) from SWETHA institute of Technology and science, Tirupati, India. Field of Interest VLSI, Embedded Systems, Scripting Languages.

 All Rights Reserved © 2014 IJARECE

Mr. R. kalyan received the B.Tech (ECE) from Sri Venkateswara College of Engineering (Autonomous) chittoor, JNTU Hyderabad, India, in 2008 and M.Tech (RF & MWE) from GITAM University, Vishakhapatnam, India, in 2010. Present He is pursuing Ph.D from jntuniversity anantapur and is currently working as an Assistant Professor in SWETHA institute of Technology and science, Tirupati, India. He has been active in research and published 3 international journals & attended 2 National conferences in the field of Communications.

V.Keerthy Rai Received the B.Tech (ECE) from saraswathi Velu College of engineering, Sholinghur, Anna University, India in 2007 and M.Tech (VLSI) from Sri Venkateswara College of Engineering (Autonomous) chittoor, JNTU Anantapur, India in 2012.And is currently working as an Assistant Professor in SWETHA institute of Technology and science, Tirupati, India. She has been active in research and published 2 international journals & attended 1 National conference in the field of Communications.