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

COPY RIGHT

IJIEMR Transactions, online available on 9th June 2017. Link :
http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-4

Title: High Security Verification of Client Intellectual Property Cores for Information Leakage.

Volume 06, Issue 04, Page No: 760-767.

Paper Authors

*PARASA ANUSHASREE, VIPPARLA RAMARAO.
* Dept. of ECE, ELURU COLLEGE OF ENGINEERING AND TECHNOLOGY.

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

HIGH SECURITY VERIFICATION OF CLIENT INTELLECTUAL PROPERTY CORES FOR INFORMATION LEAKAGE

[1]PARASA ANUSHASREE,[2] VIPPARLA RAMARAO

[1]PG Scholar, Dept. of ECE, Eluru College Of Engineering And Technology.
[2] Associate Professor, Dept. of ECE, Eluru College Of Engineering And Technology.

Anushasree.parasa@gmail.com rams404@gmail.com

ABSTRACT:The main objective of this paper is to provide stronger security for client intellectual property cores by enhancing the overall strength of the AES algorithm. Rijndael's algorithm was been selected as the Advanced Encryption Standard. The AES algorithm provides much more security without any limitations. But, recently some breaking methods on the AES have been found by cryptanalyst. For overcome this problem number of rounds in AES algorithm need to be increased. In AES algorithm, encryption and decryption involving the number of rounds depends on the length of the key and the number of block columns. So, to improve the strength of the AES the number of rounds is increased. By increasing the key length to 192 bit the strength of the AES algorithm is enhanced and in order to provide a stronger encryption method for secure communication the number of rounds is increased. In order to improve the speed of encryption and decryption code optimization is also done using the 192 bit AES.

Key Words: AES algorithm, Cryptography, Decryption, Encryption, Intellectual Property

1. INTRODUCTION

Client Intellectual Property security is becoming much more important as company spend much more time to develop it. To protect the value and ongoing usability of assets, the integrity and continuity of operations it involves all activities that institutions, enterprises and organizations undertake. Security attacks include modification of messages or files, denial of service, traffic analysis and unauthorized reading of a message of file. Computer virus is one of the most publicized types of attack on information systems. An effective network security strategy requires identification of threats and then choosing the most effective set of tools to overcome them. Security involving communications and networks is not as simple as it might first appear The expansion of the connectivity of computers makes various ways of protecting data and messages from tampering and reading. Intruders may reveal the information to an individual or organization, use it to launch an attack or modify it to misrepresent. One of the basic reasons that intruders can be successful in causing threat is that most of the information they can acquire from the system is in a form that they can read and comprehend. And one solution to this problem is by using cryptography. Cryptography ensures that the messages could not be intercepted or read by anyone other than the authorized recipient. It prevents intruders from being able to use the information that can be acquired. Thereafter, cryptography secures information by protecting its confidentiality and

can also be used to protect authenticity of data and information about the integrity.

The first encryption algorithm, Data Encryption Standard (DES) was adopted by the National Institute of Standards and Technology (NIST) to protect the confidential and sensitive information as Federal Information Processing Standard 46 (FIPS PUB 46) in 1977. However, the security of DES was reduced due to shorter length of key, existence of weak and semi-weak keys and the complementary property. Differential cryptanalysis attack is capable of breaking DES in less than 255 complexities. For differential cryptanalysis the linear cryptanalysis method can find a DES key given 243 known plain texts, as compared to 247 chosen plain texts. So, to replace the DES it was more essential to find a stronger encryption algorithm. There has been considerable interest in finding an alternative in spite of the vulnerability of DES to a brute-force attack. One approach would be to design a completely new algorithm and another alternative would be the one that preserves the existing algorithm by using multiple encryptions with ES and multiple keys. To solve the problems of DES three other algorithms were found. They are Double DES, Triple DES with two keys and Triple DES with three keys. The main drawback of Triple DES is that it has three times as many rounds as DES and hence it is much slower. Another drawback of Triple DES is it uses a 64 bit block size, because for both efficiency and security a larger block size is needed. These drawbacks of Triple DES are not favorable for long term use. The Rijndael algorithm was being adopted as an encryption standard, the Advanced Encryption System (AES) by the NIST as FIPS PUB 197 (FIPS 197) on November 2001. The AES algorithm was designed to provide more security than the DES. The AES algorithm was believed to have resistance against all known attacks, speed and code compactness on a wide range of platforms and design simplicity. AES has three variable key lengths but block length is fixed to 128 bits. The three key sizes of AES are 128, 192 and 256 bits. For an exhaustive key search AES with 128-bit keys has stronger resistance than DES.

AES implementation of 128-bit was proposed and implemented previously. This implementation for AES supports the fact that for the same algorithm different application required different implementation. Some application needs strict area requirement and a compact AES implementation will be very useful to provide security as in the some embedded system cases. On the other hand, some application highly needed the higher level of security that can be obtained without caring about the area and time limitation.

2. PROPOSED WORK

This paper shows the variation of AES algorithm called as 192 bit. The aim is to present that AES-192 bit can be used when higher level of security throughput are required without increasing overall design area as compared to the original 128 bit AES algorithm. The new algorithm consist of the structure which is similar to original AES algorithm but having slight difference that is instead of using 128 bit the plain text size and key size uses input of 192 bit that has impact on the whole algorithm structure. The AES algorithm consists of four major operations are performed during each round: byte substitution, shifting rows, mixing columns and adding the round key. AES 128 bit key is considered to be secure compared to other existing symmetric cipher algorithm. It is widely used in many applications where the security is most important. The new AES algorithm provides even more security and

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

double throughput. More security comes from using larger key size and more throughputs come from using four times larger block size that the block size used in the original AES.

The proposed AES 192 algorithm has four main different byte based transformation. The first transformation is the byte substitution which substitutes the value of 192 bit and this is achieved by using parallel s-boxes. The second transformation is shifting rows that shift the rows of the output from previous step by an offset equal to the row numbered. The third transformation is mixing column, where each column of the output from previous step is multiplied by different value. The final transformation in the round is adding round key to the result of this round.The top level architecture of the AES-192 bits is shown in Figure 1. The plaintext is 128-bit and the key size 192-bit. The AES-192 algorithm processes the data in 10 rounds. The key and the input data are loaded when the Load key control signal is one and zero, respectively. The Encrypt signal starts the encryption process, while reset resets everything to zero. The resulting cipher text is also 128-bits. More details about each of the transformations used in the AES-192 are described in the coming subsections. Where the key expansion procedure is explained later since each round needs its own key generated according to this procedure.

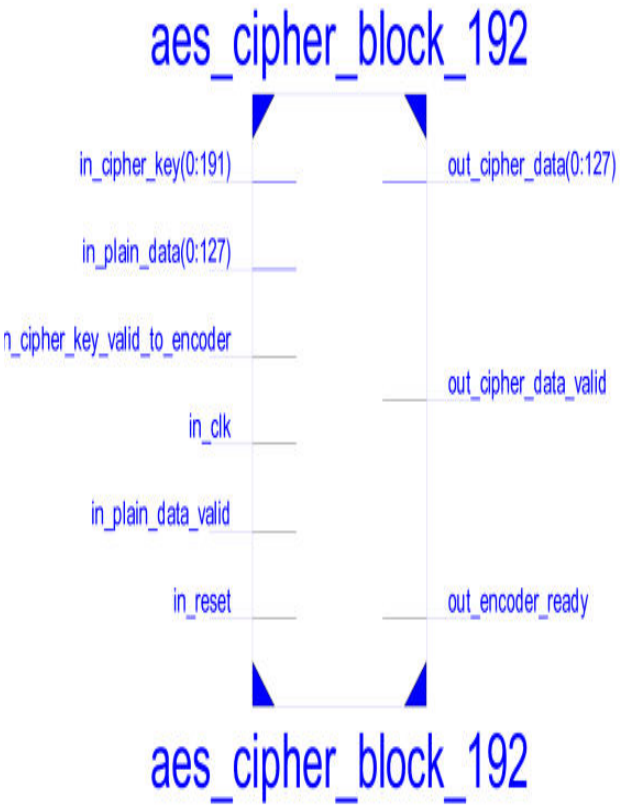


Figure 1

3. IMPLEMENTATION OF ENCRYPTION

The input key for encryption is 192 bits. The cipher is specified in terms of repetitions of processing steps that are applied to make up rounds of keyed transformations between the input plaintext and the final output of cipher-text. The encryption procedure of AES 192 has been illustrated in figure 2.Each round in AES 192 encryption includes four different round transformations namely Substitute Bytes, Shift Rows, Mix Columns and Add Round Key. The last round of AES 192 encryption alone does not include the Mix Columns transformation.

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

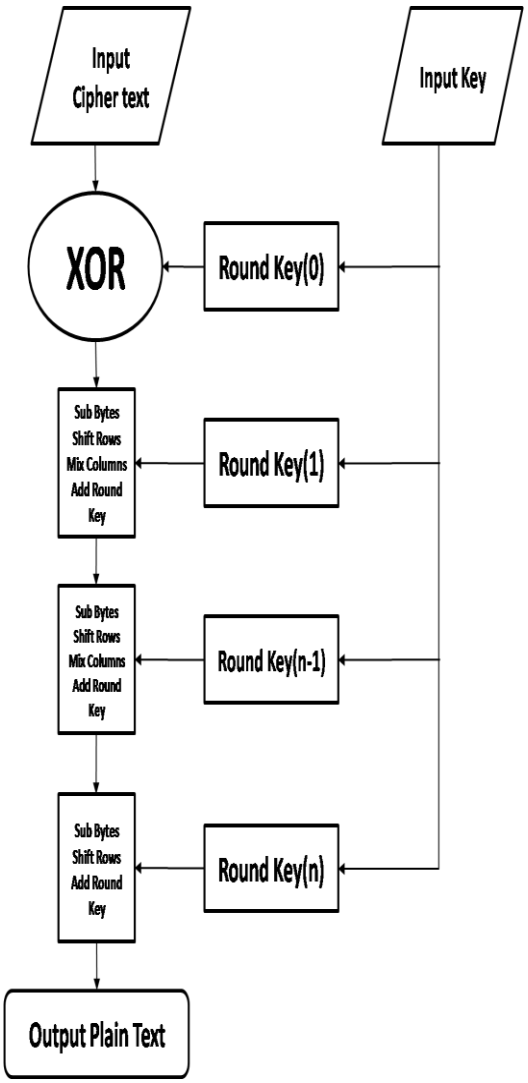


Figure 2

4. IMPLEMENTATION OF DECRYPTION

A set of reverse rounds are applied to transform cipher text back into the original plain-text using the same encryption key. The four reverse transformations used are Add Round Key, Inverse Mix Columns, Inverse Shift Rows and Inverse Substitute Bytes. Each round in decryption of AES 192 includes all the four reverse transformations except in the first round. The Inverse Mix Column transformation is violated in the first round of decryption since it does not occur in the last round of encryption.

The decryption procedure of AES 192 is illustrated in figure 3.

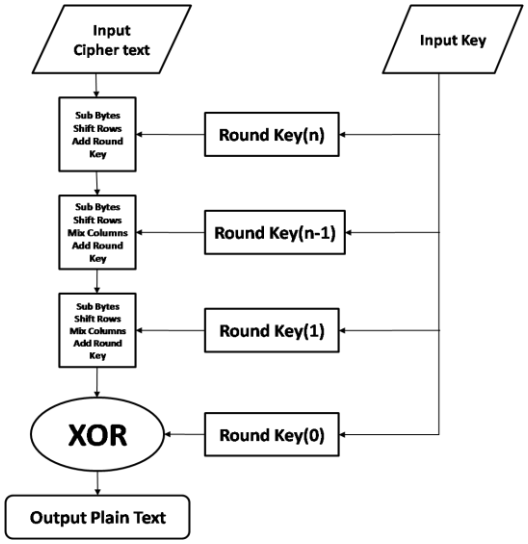


Figure 3

5. STAGES IN ENCRYPTION AND DECRYPTION

➢ Byte Substitution

The 512-bits input plaintexts are organized in array of 64-bytes and are substituted by values obtained from Substitution boxes. This is done (as in the original AES) to achieve more security according to diffusion-confusion Shannon's principles for cryptographic algorithms design. To overcome the overhead of the huge data size used (512-bits), the Substitution boxes are implemented as lookup tables, and accessed in parallel as shown in Figure 4.

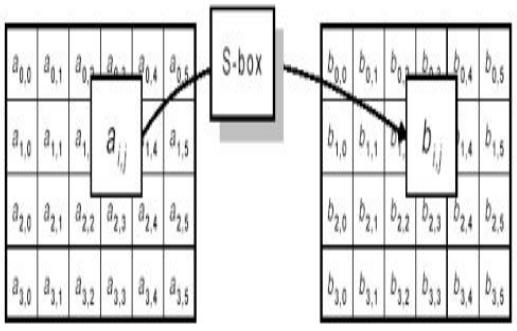


Fig -4: Byte Substitution

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

➢ Shift Row

After the original 192-bit data is substituted with values from the S-boxes, the rows of the resulting matrix are shifted in a process called Shift Row transformation. What happened in this part is that the bytes in each row in the input data matrix will be rotated left. The number of left rotations is not the same in each row, and it can be determined by the row number. For example, row number zero is not shifted; the first row is shifted by one byte, and so on.

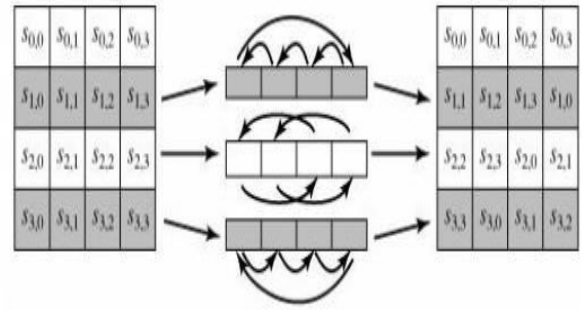


Fig -5: Shift Row

➢ Mix Column

Now, and after the rows of the input data are rotated left by different offsets, an operation must be applied to the columns of the data matrix. The Mix Column transformation multiplies the columns of the data matrix by a pre-defined matrix. The AES-192 and original AES process the data in bytes basis. Each byte is considered as polynomials over GF (2^8) with 8 terms. To explain how the Mix Column works, we have to explain the concept of polynomials over GF (2^n) in general and for GF (2^8) as example when n=8. The conversion might be dictated by the accompanying grid increase on state. Every component of the item framework is the entirety of results of components of one line and one segment. For this situation the unique augmentations & multiplication are achieved in GF (2^8).

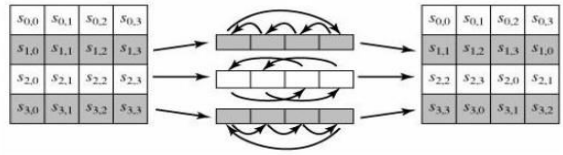


Fig -6: Mix Column

➢ Add Round Key

In this process, the 128 bits of state are bitwise XORed through the 128 bits of the round key. The procedure is seen as a column wise process between the word of a state column and one WORD of the round key. This conversion is as basic as would be prudent which benefits in effectiveness yet it additionally influences all of state. To make the relationship between the key and the cipher text more complicated and to satisfy the confusion principle, the Add Round Key operation is performed. This addition step takes the resulting data matrix from the previous step and performs on it a bitwise XOR operation with the sub key of that specific round (addition operation in GF (2n)).

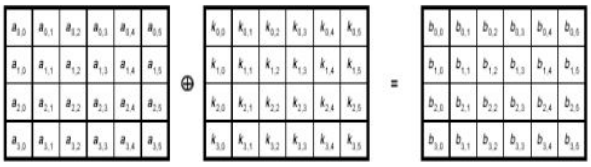


Fig -7: Add Round Key

6. COMPARASION OF AES 128 AND AES 192

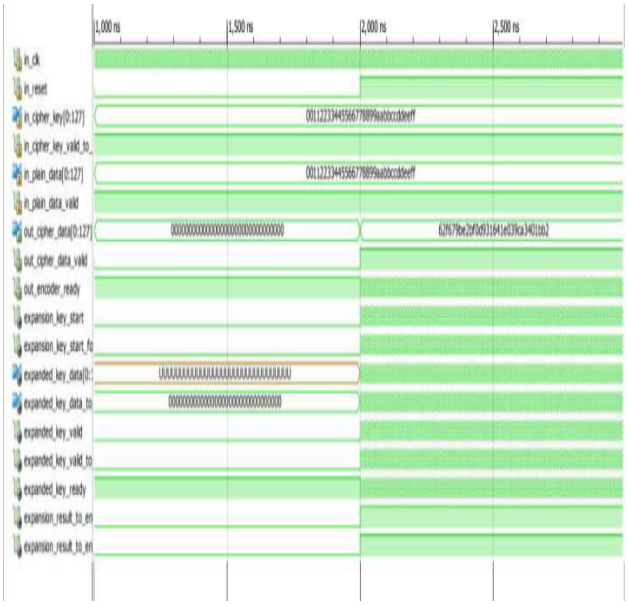
The performance of 128 bit AES algorithm is compared with the performance of AES 192 algorithm. Encryption and decryption of AES 128 is implemented to compare it with AES 192. In terms of security the 128 bit AES algorithm is weaker than the 192 bit AES algorithm. This is because the length of the key used in 192 bit AES increases the number of rounds for both encryption and decryption. But when the number of rounds increases, the encryption and decryption procedures become

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

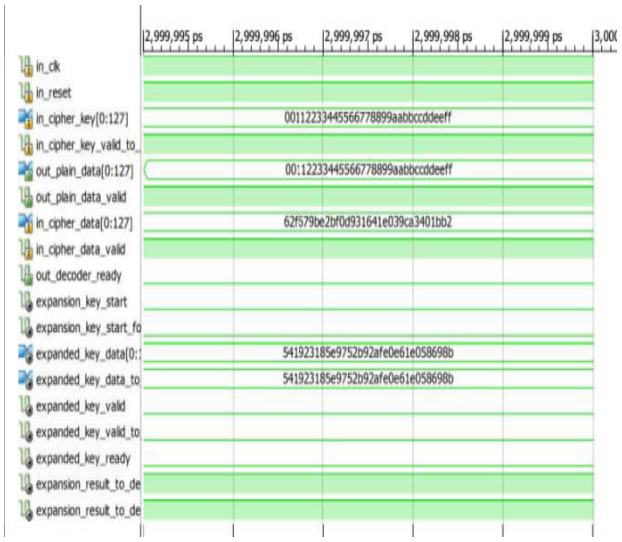
more complex thereby degrading the speed of the 192 bit AES algorithm. Thus there is a tradeoffs between speed and security. The performance is compared in terms of time taken. The time taken for encryption and decryption of AES 128 bit and AES 192 bit are noted to measure their speed. The system time is noted at the start of encryption process and the end time, after encryption completes is also noted. The same process is repeated for decryption also to calculate the time taken for decryption.

Parameters	AES 128-bit	AES 192-bit
Key Size	128-bit	192-bit
Data Block Size	Size same as Key	Size not-same as Key
Rounds	10	12
Throughput	Less	More
Security	Less	More
Processor Required	More	Less

7. SIMULATION RESULTS



Encryption of data using AES



Decryption of data using AES

8. CONCLUSION

We proposed a new variation of AES-192 with 128-bit input block and 192-bit key size compared with 128-bit in the original AES-128 algorithm. When the number of rounds is increased, it improves the complexity of the algorithm making it stronger against the cryptographic attacks. However the length of the key is increased as number of rounds depend on the length of the key used in order to increase the number of rounds involved. Thus the increase in length of the key gives the AES algorithm a strong resistance against the new attacks and has an acceptable speed of data encryption and decryption. A complete XILINX implementation for the new AES-512 was also presented in this paper. After comparing the implementation results, we found that our new design has increased throughput compared with the original AES-128 design. The larger key size makes the algorithm more secure, and the larger input block increases the throughput. The extra increase in area can be accepted and makes the proposed algorithm ideal applications in which high level of security and high throughputs are required.

REFERANCES

[1] "Defense Science Board (DSB) study on High Performance Microchip Supply," http://www.acq.osd.mil/dsb/reports/ADA435563.pdf, 2005.

[2] S. Bhunia, M. Hsiao, M. Banga, and S. Narasimhan, "Hardware Trojan Attacks: Threat Analysis and Countermeasures," Proceedings of the IEEE, vol. 102, no. 8, pp. 1229–1247, 2014.

[3] M. Tehranipoor and F. Koushanfar, "A Survey of Hardware Trojan Taxonomy and Detection," IEEE Design and Test of Computers, vol. 27, no. 1, pp. 10–25, 2010.

[4] X. Zhang and M. Tehranipoor, "Case study: Detecting hardware Trojans in third-party digital IP cores," IEEE Intentional Symposium on Hardware Oriented Security and Trust, pp. 67–70, 2011.

[5] M. Banga and M. Hsiao, "Trusted RTL: Trojan detection methodology in pre-silicon designs," IEEE International Symposium on HardwareOriented Security and Trust, pp. 56–59, 2010.

[6] J. Jou and C. J. Liu, "Coverage analysis techniques for HDL design validation," IEEE Asia Pacific Conference on Chip Design Languages,1999.

[7] H. Salmani and M. Tehranipoor, "Analyzing circuit vulnerability to hardware Trojan insertion at the behavioral level," IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems, pp. 190–195, 2013.

[8] A. Waksman, M. Suozzo, and S. Sethumadhavan, "FANCI: Identification of Stealthy Malicious Logic Using Boolean Functional Analysis," ACM Conference on Computer and Communications Security, pp. 697– 708, 2013.

[9] J. Zhang, F. Yuan, L. Wei, Z. Sun, and Q. Xu, "VeriTrust: Verification for hardware trust," IEEE/ACM Design Automation Conference, pp. 1– 8, 2013.

[10] J. Zhang, F. Yuan, and Q. Xu, "DeTrust: Defeating Hardware Trust Verification with Stealthy Implicitly-Triggered Hardware Trojans," ACM Conference on Computer and Communications Security, pp. 153–166, 2014.

[11] E. Love, Y. Jin, and Y. Makris, "Proof-Carrying Hardware Intellectual Property: A Pathway to Trusted Module Acquisition," IEEE Trans. on Information Forensics and Security, vol. 7, no. 1, pp. 25–40, 2012.

[12] Y. Jin and Y. Makris, "Proof carrying-based information flow tracking for data secrecy protection and hardware trust," IEEE VLSI Test Symposium, pp. 252–257, 2012.

[13] "A proof-carrying based framework for trusted microprocessor IP," IEEE/ACM International Conference on Computer-Aided Design, pp. 824–829, 2013.

[14] Jasper, "JasperGold: Security Path Verification App," http://www. jasper-da.com/products/jaspergold-apps/security path verification app, 2014.

[15] P. Subramanyan and D. Arora, "Formal verification of taint-propagation security properties in a commercial SoC design," Design, Automation and Test in Europe Conference and Exhibition, pp. 1–2, 2014.

[16] J. Rajendran, V. Vedula, and R. Karri, "Detecting Malicious Modifications of Data in Third-party Intellectual Property Cores," IEEE/ACM Annual Design Automation Conference, pp. 112:1–112:6, 2015.

[17] J. Woodcock, P. G. Larsen, J. Bicarregui, and J. Fitzgerald, "Formal Methods: Practice and Experience," ACM Computing Surveys, vol. 41, no. 4, pp. 19:1–19:36, 2009.

[18] A. Pnueli, "The temporal semantics of concurrent programs," Semantics of Concurrent Computation, vol. 70, pp. 1–20, 1979.

[19] "Cadence: Smv," http://www.cadence.com/products/fv/pages/default.aspx, 2005.

[20] A. Biere, A. Cimatti, E. Clarke, and Y. Zhu, "Symbolic Model Checking without BDDs," Tools and Algorithms for the Construction and Analysis of Systems, vol. 1579, pp. 193–207, 1999.

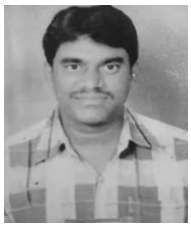
[21] L. Feiten, M. Sauer, T. Schubert, A. Czutro, E. Bohl, I. Polian, and B. Becker, "#SAT-based vulnerability analysis of security components — A Case Study," IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems, pp. 49–54, 2012.

[22] H. Eldib, C. Wang, and P. Schaumont, "SMT-Based Verification of Software Countermeasures against Side-Channel Attacks," International Conference on Tools and Algorithms for the Construction and Analysis of Systems, pp. 62–77, 2014.

[23] M. Tehranipoor, R. Karri, F. Koushanfar, and M. Potkonjak, "Trusthub," http://trust-hub.org.

AUTHORS:

Parasa Anushasree is PG Scholar perusing her M.Tech and received her B.Tech degree from in Eluru college of engineering and technology, India in Electronics and Communications Engineering. Her area of interests include VLSI, Data processing, Cryptography and Information Security.



Vipparla Ramarao received his M.Tech degree from JNTUH,HYD,India and B.Tech degree from Mallineni Lakshmaiah Engineering college, Prakasam Dt., India in Electronics and Communications Engineering. He is currently working as Associate Professor in Eluru college of engineering and technology, Eluru, India. His area of interests include VLSI,image processing, Data Mining and Information Security.