DESIGN OF RELIABLE CRC ERROR DETECTION FOR SERIAL FINITE FIELD MULTIPLIERS FOR CRYPTOGRAPHY APPLICATIONS

[1] CH. KUTUMBA RAO, M.Tech, Y.BARNABAS WESLY [2].

[1] ASSOCIATE PROFESSOR OF ECE IN SREE VAHINI INSTITUTE OF SCIENCE & TECHNOLOGY TIRUVURU, KRISHNA DIST. 521235, AP, INDIA.

[2] PG STUDENTS FROM DEPT OF ECE IN SREE VAHINI INSTITUTE OF SCIENCE & TECHNOLOGY TIRUVURU, KRISHNA DIST. 521235, AP, INDIA.

ABSTRACT

Finite-field multiplication plays vital role in literature with applications in cryptography and error-detecting codes. In many cryptographic algorithms this arithmetic operation is a complex, costly, and time-consuming task that may require millions of gates. In this work, we propose efficient hardware architectures based on cyclic redundancy check (CRC) as error-detection schemes for post quantum cryptography (PQC) with case studies for the Luov cryptographic algorithm. We have developed verification codes through which software implementations of the proposed schemes are performed to verify the derivationsof the formulations. Additionally, verifying that the proposed schemes achieve high error coverage with acceptable overhead.

Index Terms*: Cyclic Redundancy Check (CRC) Finite-field multiplication, Post Quantum Cryptography.*

I.INTRODUCTION

Very-large-scale integration (VLSI) is the process of creating an integrated circuit (IC) by combining thousands of transistors into a single chip. VLSI began in the 1970s when complex semiconductor and communication technologies were being developed. The microprocessor is a VLSI device. Before the introduction of VLSI technology, most ICs had a limited set of functions they could perform. An electronic circuit might consist of a CPU, ROM, RAM and other glue logic. VLSI lets IC designers add all of these into one chip. The electronics industry has achieved a phenomenal growth over the last few decades, mainly due to the rapid advances in large scale integration technologies and system design applications.

With the advent of very large scale integration (VLSI) designs, the number of applications of integrated circuits (ICs) in high-performance computing, controls, telecommunications, image and video processing, and consumer electronics has been rising at a very fast pace.

In the modern time, integrated circuit (chip) is widely applied in the electronic equipment. Almost every digital appliance, like computer, camera, music player or mobile phone, has one or several chips on its circuit board. Very Large Scale Integration (VLSI), in general, comprises over an excess of one million transistors, an incredible figure that could not have been imagined a decade ago. Though the complexity of the chip has compounded by a factor of 1000 since its first introduction, yet the term VLSI still remains to be accepted and denotes digital integrated systems with high complexity. Further, past few decades have witnessed an extraordinary increase in VLSI research. The Computer-Aided Design (CAD) has further aided the growth in the complexity and performance of integrated circuits in the VLSI technology. With such a phenomenal increase in complexity, it is more crucial than ever before to manage the design process, in order to maintain the reliability, quality, and extensibility of a given design The process includes "definition, execution and control of design methodologies in a flexible and configurable way". Speed of development in high-performance computing, for the telecommunications and consumer for the electronics in a rapidly changing market, developmental costs, and cost involved in case of mistakes, play a critical role in a commercial environment. Hence, it requires designs that can be processed quickly, cheaply and mistakes brought to the forefront at the earliest, perhaps, before fabrication stage. VLSI is preferred due to its many advantages: compactness, less area, physically smaller; higher speed, lower parasitic (reduced interconnection length); lower power consumption; and higher reliability, improved on-chip interconnects. In addition, VLSI integration significantly reduces manufacturing cost. Nevertheless, a few disadvantages, such as long design and fabrication time and higher risk to project with complexity of millions of components leads to the anticipation of fast computation and layouts close to optimality generation. The research and development of circuit layout (Physical Design) automation tools could pave a way for future growth of VLSI systems. The accepted norm about the

layout of integrated circuits on chips and boards is that it is a complex process. Consequently, any problem arising as a result of optimization problems requires to be solved during the circuit layout, which is intractable. This refers to the fact that they are mostly Nondeterministic Polynomial (NP) - hard. The major implication of this recourse is that the optimal solutions cannot be achieved in polynomial time.

II.LITERATURE SURVEY

Reliable architecture-oblivious error detection schemes for secure cryptographic GCM structures, In this paper, we proposed, simulated through error injections, and implemented on ASIC our proposed schemes for the GCM. Our schemes constitute algorithm-oblivious constructions through RESCAB, which can be applied to the GCM architectures using different finite field multipliers in GF (2128); for example, in our experiments, we used a quadratic and a sub quadratic multiplier to show the obliviousness of the proposed approach. The proposed scheme is not limited to the types of finite field multipliers, can be tailored towards higher reliability or lower overhead, can be applied to different block ciphers, and considers biased fault models. Such obliviousness for the proposed constructions used in the GCM gives freedom to the designers. Through deep sub pipelining, we reached an area overhead of 6.7% and a throughput degradation of 7.7%. Moreover, for RESCAB 225 cycles (210 cycles), we reached an area overhead of 4.9%, while throughput degradations are 11.9% and 8.5%, respectively. Based on the available resources, one may utilize the proposed error detection schemes for making the hardware implementations of the GCM more reliable. A. Sarker, M. Mozaffari-Kermani, and R. Azarderakhsh, “Hardware constructions for error detection of number-theoretic transform utilized in secure cryptographic architectures,” In this paper, we have presented a number of categories for error detection schemes of NTT in the ring R = (Z/ pZ[x]/xn +1), which are also platform-oblivious. The proposed schemes constitute error detection architectures on hardware based on recomputation with encoded operands. Our target has been low hardware overhead, which is favorable to compact and deeply embedded architectures. We have implemented the proposed error-detection techniques on ASIC for a 65-nm library to assess the implementation and performance metrics. With high error coverage, the presented approaches achieve an acceptable overhead (at most 24% area,

18% power consumption, and 9% delay for the synthesized case studies) and can be tailored toward the objectives in terms of error detection and reliability.M. Mozaffari-Kermani, R. Azarderakhsh, and A. Aghaie, "Fault detection architectures for post-quantum cryptographic stateless hash-based secure signatures benchmarked on ASIC," Post-quantum cryptographic implementation attacks and natural faults need to be detected through efficient countermeasures. In this article, various fault diagnosis approaches for hash-based post-quantum signatures are proposed. The merit of the proposed schemes is that they are a step forward towards reliability and fault attack immunity of resistant hash trees in future potential post-quantum systems. Based on the reliability requirements and available resources, one may select the error detection schemes suitable for these architectures. We have developed a method for swapping nodes and leaves in binary hash trees, L-Trees, and Merkle trees to detect faults, where recomputations with rotated/shifted, and, in general, encoded operands fail. We have also discussed various complications in special hash tree constructions. Moreover, for the inner hash functions BLAKE and SPONGENT, we have presented a number of diagnosis methods that are capable of reaching high error coverage (this includes analysis of false alarms) with acceptable area overhead and performance degradation. M.Mozaffari-Kermani and R. Azarderakhsh, "Reliable hash trees for post quantum stateless and cryptographic hash-based signatures," in Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst. (DFTS),Oct. 2015, pp. 103–108. In this paper, two fault diagnosis approaches for hash based post-quantum signatures are proposed. The merit of the proposed schemes is that they are a step-forward towards reliability and fault attack immunity of resistant hash trees in future potential post quantum systems. We have developed a method for swapping nodes and leaves in binary hash trees, LTrees, and Merkle trees to detect faults, where recomputations with rotated/shifted, and in general, encoded operands fail. Moreover, for the inner hash function, we have presented two diagnosis methods which are capable of reaching high error coverage with acceptable area overhead and performance degradation. Based on the reliability requirements and available resources, one may select the error detection schemes suitable for these architectures. Finally, in this paper, we have considered hash-based signature schemes as one potential method for post-quantum

cryptography. An intriguing future investigation is developing post-quantum resistant and reliable architectures through code based, lattice-based, and multivariate-quadratic equations, and ideally introducing a new metric which benchmarks post quantum architecture reliability and fault attack immunity

III. EXISTING SYSTEM: PARITY PREDICTION

Finite-field multipliers perform Finite-field multiplication modulo, an irreducible polynomial used to define the finite field. For post quantum cryptography (PQC), the inputs can be very large, and the finite-field multipliers may require millions of logic gates. Finite field multiplication is quite different from its counterparts in integer and floating point number systems. For today's cryptographic applications, the field size can be very large and each input of the multiplier can be 160 to 2048 bits long. Such a multiplier may require millions of logic gates and it is a challenging task to implement it free of faults. If one can have a multiplier which is capable of detecting error on-line at the presence of certain faults, cryptographic schemes can be operated morereliably. The importance of eliminating errors in cryptographic computations has been pointed out in some recent articles. The presence of faults in cryptosystems can lead to an active attack and the simplest way to prevent such an attack is to ensure that the computational device verifies the values it computes before sending them out. In an attempt to detect errors in finite field multipliers, have considered bit-serial multipliers in GF(2m) and have presented error detection schemes for four types of multipliers using a parity prediction technique. Their polynomial basis scheme for error detection is applicable to a special class of fields. These fields are defined using irreducible all-one polynomials that are available for certain values of m only. Additionally, when an all-one polynomial is irreducible, the corresponding m is not a prime. This makes many designers to avoid such a value of m and the corresponding irreducible all-one polynomial that define the underlying field for certain cryptosystems, such as those based on elliptic curve cryptography. The polynomial basis is used for representing the field elements. We investigate error detection techniques for such multipliers and develop parity prediction based error detection schemes for both bit-serial and bit-parallel multipliers. The new schemes can be used

for any field defining irreducible binary polynomial.

In many of cryptographic schemes, the most time consuming basic arithmetic operation is the finite field multiplication and its hardware implementation may require millions of logic gates. It is a complex and costly task to develop such large finite field multipliers which will always yield error free outputs. In this effect, this considers fault tolerant multiplication in finite fields. It deals with detection of errors of bit-parallel and bit serial polynomial basis multipliers over finite fields of characteristic two. Our approach is to partition the multiplier structure into a number of smaller computational units and use the parity prediction technique to detect errors. Error detection schemes for GF(2m) multiplication operation that relies on the architecture A bit-parallel architecture for GF(2m) multiplication. It mainly consists of three types of modules, namely, sum, pass-thru and α modules. The sum module (denoted as a double circle with a plus inside) is to simply add two GF(2m) elements and it can be realized in hardware using m two-input XOR gates. The pass-thru module (denoted as a double circle with a dot inside) is to multiply a GF(2m) element by a GF(2) element, i.e., if X(i) ∈ GF(2m) and bi ∈ GF(2) are two inputs to a pass-thru module, the third module (i.e., the rectangular shape α module) multiplies its input, which is an element of GF(2m), by α and reduces the result modulo F(α).

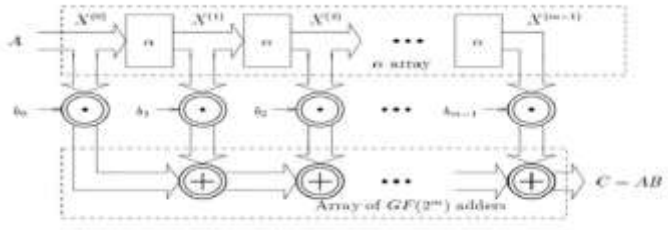

Figure 1: Multiplication of2 elements in GF (2^m).

IV.PROPOSED SYSTEM: CRC ERROR-DETECTION SCHEME

CYCLIC REDUDANCY CHECK (CRC) error-detection scheme result provides a broader and higher error coverage than parity signatures and explore the application of such schemes to the Luov algorithm. We derive and apply CRC signatures to the finite-field multipliers used in Luov algorithm. This would be a step forward toward detecting natural and malicious intelligent faults, especially and as discussed in this brief, considering both primitive and standardized CRCs with different fault multiplicity coverage. CRC

was first proposed in 1961 and it is based on the theory of cyclic error-correcting codes. To implement CRC, a generator polynomial g(x) is required.

These finite-field multiplications are very complex and require large-area footprint. Therefore, it is a complex task to implement such architectures resilient to natural and malicious faults. The aim of this work is to provide countermeasures against natural faults and fault injections for the finite-field multipliers used in cryptosystems such as the Luov algorithm as a case study, noting that the proposed error-detection schemes can be adapted to other applications and cryptographic algorithms whose building blocks need finite-field multiplications this process takes place as shown in figure.

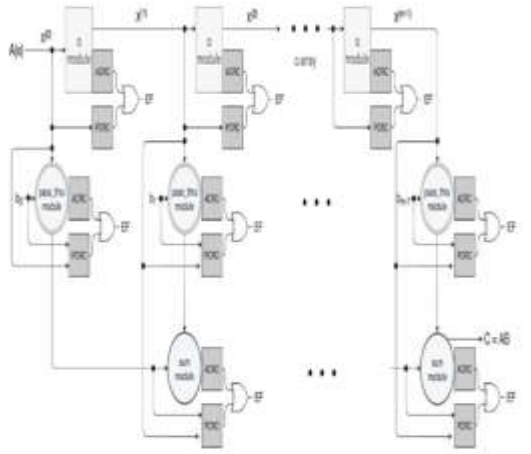

Figure 2: Finite-field multiplier with the proposed error-detection schemes based on CRC

To perform multiplication, three different modules are needed: sum, α, and pass-thru modules. The sum module adds two elements in G F(2m) using m two-input XOR gates, the α module multiplies an element of G F(2m) by α and then reduces the result modulo f (x), and lastly, the pass-thru module multiplies a G F(2m) element by a G F(2) element. One finite-field multiplication uses a total of m − 1 sum modules, m − 1 α modules, and m pass-thru modules to get the output. Fault injection can occur in any of these modules, and formulations for parity signatures in GF(2m). Parity signatures provide an error flag (EF) on each module. The major drawback of parity signatures is that their error coverage is approximately 50%, that is, if the number of faults is even, the approach would not be able to detect the faults. This highly predictable countermeasure can be circumvented by intelligent fault injection. In this work, our aim is the derivation of error-detection schemes that provide a broader and higher error coverage than parity signatures and explore the application of such schemes to the Luov algorithm. CRC was first proposed in 1961 and it is based on the theory of cyclic error correcting codes. To implement CRC, a generator polynomial g(x) is required. The

message becomes as the dividend, the quotient is discarded, and the remainder produces the result. In CRC, a fixed number of check bits are appended to the data and these check bits are inspected when the output is received to detect any errors. The entire finite-field multiplier with our error-detection schemes is shown in Fig. 3, where actual CRC (ACRC) and predicted CRC (PCRC) stand for ACRC signatures and PCRC signatures, respectively. In Fig. 3, only one EF is shown for clarity; however, for CRC-5, which is the case study proposed in this brief,5 EFs are computed on each module. In Fig. 3, the α module is shown more in-depth to clarify how the proposed CRC signatures work in each finite-field multiplier. For the sum and pass-thru modules, it follows the approach as for parity signatures described in [16]. For the sum module in CRC-1, pˆx is equal to the sum of the parity bits of the input elements A and B in G F(2m), pˆX = pA + pB. Furthermore, for the pass-thru module in CRC-1, pˆX = b· pA, where b is an element in GF(2). For any other CRC-n scheme, instead of summing all the bits, it checks n bits at a time in the sum and pass-thru modules.

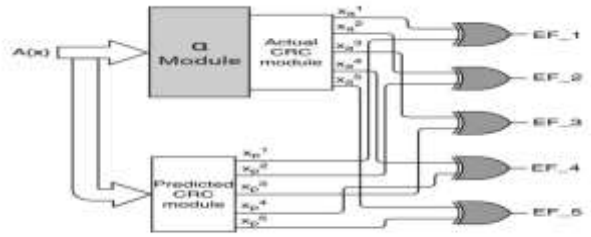

Figure 3: Proposed error-detection constructions for α module

The predicted output and the actual output are divided into five parity groups respectively. These parity groups are XORed with each other to determine if there has been any fault, for example, flip of bits, during the α module operation. In total, each α module outputs five EFs. Fig. 3 shows the implementation of the α module with the proposed error detection schemes. A(x) is the input with the form p(x) = a^m−1x^m−1 + ⋯ + a1x + a0, which goes to two different modules that run in parallel. In the α module, (1) takes place. The output from the α module is divided into five groups in the ACRC module, which are denoted as x1 a – x5a in Fig. 2. Meanwhile, A(x) is also being divided into five groups in the PCRC module, which are denoted as x1 p–x5 p. Once the two CRC modules are done, each group is XORed with its respective one to produce five EFs, which are represented as E F1– E F5. For our case study, the outputs are divided into five groups since we use CRC-5; however, if any other CRC-n is used, there will be n EFs and the actual and

predicted outputs will be divided into n groups.

V. SIMULATION RESULTS

This is a RTL Schematic for proposed system i.e CRC error detection is drawn in XILINX ISE tool as shown in figure 4

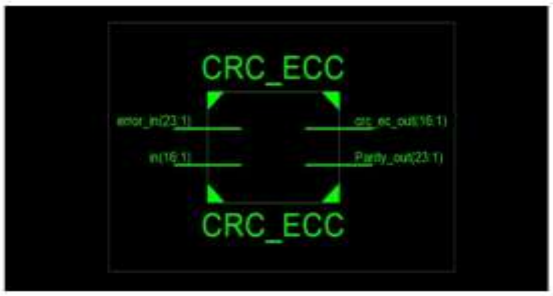

Figure: 4 RTL Schematic

This is the inner RTL schematic for proposed CRC error detection is shown in figure 5

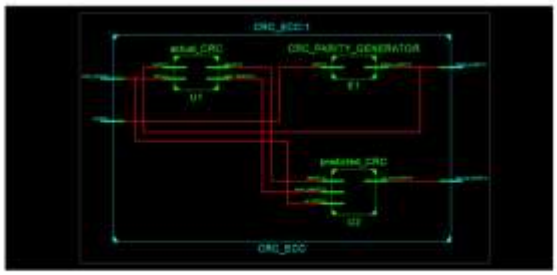

Figure 5: Inner RTL Schematic

The output wave forms are shown in the figure 6 for CRC error detection

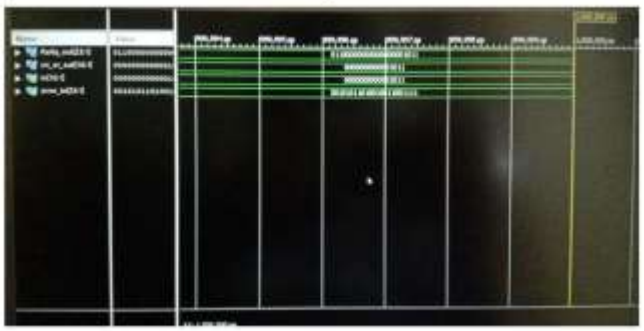

Figure 6: output wave forms

PARAMETERS	EXISTING METHOD	PROPOSED METHOD
Area (No.of slices)	178	18
Delay (ns)	5.841	1.5
Power (W)	2.93	0.073

Table 1: comparison synthesis report

VI. CONCLUSION

Derived error detection schemes for the finite-field multipliers used in post quantum

cryptographic algorithms such as Luov, noting that the proposed error- detection schemes can be adapted to other applications and cryptographic algorithms whose building blocks need finite-field multiplications. The error-detection architectures proposed in this work are based on CRC-5 signatures and we have performed software implementations for the sake of verification. Additionally, we have explored and studied both primitive and standardized generator polynomials for CRC-5, comparing the complexity for each of them. We have embedded the proposed error-detection schemes into the original finite-field multipliers of the Luov's algorithm, obtaining high error coverage with acceptable overhead.

Future scope: In future the proposed error-detection schemes into the original finite-field multipliers of the Luov's algorithm, obtaining high error coverage with acceptable overhead.

REFERENCES

[1] Alvaro Cintas Canto , Mehran Mozaffari-Kermani,and Reza Azarderakhsh, Reliable CRC-Based Error Detection Constructions for Finite Field Multipliers With Applications in Cryptography, published in IEEE transactions on very large scale integration (VLSI) systems, vol. 29, no. 1, January 2021.

[2] J. L. Danger et al., "On the performance and security of multiplication in G F(2N)," Cryptography, vol. 2, no. 3, pp. 25–46, 2018

[3] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "Reliable hardware architectures for the third-round SHA-3 finalist Grostl benchmarked on FPGA platform," in Proc. DFT, Oct. 2011, pp. 325–331.

[4] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "A low-cost S-box for the advanced encryption standard using normal basis," in Proc. IEEE Int. Conf. Electro/Inf. Technol., Jun. 2009, pp. 52–55.

[5] M. Yasin, B. Mazumdar, S. S. Ali, and O. Sinanoglu, "Security analysis of logic encryption against the most effective side-channel attack: DPA," in Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst. (DFTS), Oct. 2015, pp. 97–102.

[6]M Mozaffari-Kermani, R. Azarderakhsh, A. Sarker, and A. Jalali, "Efficient and reliable error detection architectures of hash-counter-hash tweakable enciphering schemes," ACM Trans. Embedded Comput.

Syst., vol. 17, no. 2, pp. 54:1–54:19, May 2018.

[7]M.Mozaffari-Kermani, R. Azarderakhsh, and A. Aghaie, "Reliable and error detection architectures of Pomaranch for false-alarm-sensitive cryptographic applications," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 23, no. 12, pp. 2804–2812, Dec. 2015.

[8] A. Sarker, M. Mozaffari-Kermani, and R. Azarderakhsh, "Hardware constructions for error detection of number-theoretic transform utilized in secure cryptographic architectures," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 27, no. 3

[9] M. Mozaffari-Kermani, R. Azarderakhsh, and A. Aghaie, "Fault detection architectures for post-quantum cryptographic stateless hash-based secure signatures benchmarked on ASIC," ACM Trans. Embedded Comput. Syst., vol. 16, no. 2, pp. 59:1–59:19, Dec. 2016.

[10]M. Mozaffari-Kermani and R. Azarderakhsh, "Reliable hash trees for post-quantum stateless cryptographic hash-based signatures," in Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst. (DFTS), Oct. 2015, pp. 103–108.

[11] M. M. Kermani and R. Azarderakhsh, "Reliable architecture-oblivious error detection schemes for secure cryptographic GCM structures," IEEE Trans. Rel., vol. 68, no. 4, pp. 1347–1355, Dec. 2019.

[12]A.A.Kamal and A. M. Youssef, the "Strengthening hardware implementations of NTRUEncrypt against fault analysis attacks," J. Cryptograph. Eng., vol. 3, no. 4, pp. 227– 240, Nov. 2013.

[13] A. Kipnis, J. Patarin, and L. Goubin, "Unbalanced oil and vinegar signature schemes," in Proc. Int. Conf. Theory Appl. Cryptograph. Techn. Berlin, Germany: Springer, 1999, pp. 206–222.

[14] D. Moody, "Post-quantum cryptography: NIST's plan for the future," Tech. Rep., Feb. 2016.

[15] D. Moody, "Post-quantum cryptography: Round 2 submissions," Tech. Rep., Mar. 2019.

[16]D.J.Bernstein,"Post-quantumcryptography," in Encyclopedia of Cryptography and Security, H. C. A. van Tilborg and S. Jajodia, Eds. Boston, MA, USA: Springer, 2011, pp. 949–950, doi: 10.1007/978-1-4419-5906- 5_386.

[17] A. Reyhani-Masoleh and M. A. Hasan, "Error detection in polynomial basis multipliers over binary extension fields," in Proc. CHES, 2002, pp. 515–528.

[18] EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz 960 MHz, EPC Global, Brussels, Belgium, Version 1.0.23, 2008.

[19] T. V. Ramabadran and S. S. Gaitonde, “A tutorial on CRC computations,” IEEE Micro, vol. 8, no. 4, pp. 62–75, Aug. 1988.

[20] S. Subramanian, M. Mozaffari-Kermani, R. Azarderakhsh, and M. Nojoumian, “Reliable hardware architectures for cryptographic block ciphers LED and HIGHT,” IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 36, no. 10, pp. 1750–1758, Oct.

BIBLIOGRAPHY

AO, M.Tech, Working as an Associate Professor of ECE in Sree Vahini Institute of S gy Tiruvuru, Krishna Dist. 521235, AP, India.

Y.BARNABAS WESLY, studying M.Tech in VLSI & ES in Sree Vahini Institute of Science & Technology Tiruvuru, Krishna Dist. 521235, AP, and India.