International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

A TRUSTWORTHY CYCLIC REDUNDANCY–ORIENTED ERROR CONTROL SCHEME FOR FINITE FIELD MULTIPLIERS IN CRYPTOGRAPHIC ENGINES

D. DILEEP [1],CHELLETI SIVA NAGA PRASAD[2], SINGAREDDY JAY VARUN[3],NAGANABOINA DHANA KIRAN[4],KARETI SAI CHANDU[5]
[1]AssistantProfessor, Dept. of ECE, V.K.R., V.N.B. & A.G.K. COLLEGE OF ENGINEERING, GUDIVADA.
[2345]UG Students, Dept. of ECE, V.K.R., V.N.B. & A.G.K. COLLEGE OF ENGINEERING, GUDIVADA.

ABSTRACT
Finite-field multiplication plays a critical role in encryption and error-detecting codes, yet it remains a computationally intensive and hardware-expensive operation, often requiring millions of logic gates for modern cryptographic algorithms. This paper presents a case study of the Luov cryptographic algorithm and proposes a hardware architecture leveraging cyclic redundancy check (CRC) for error detection in post-quantum cryptography (PQC) applications. The selected CRC polynomials offer robust error-detection capabilities and are well-suited for the specified field widths. To validate the correctness of the proposed schemes, we develop verification algorithms that facilitate software-based testing. Hardware implementations of the original multipliers on a Xilinx field-programmable gate array (FPGA) confirm that the proposed error-detection techniques achieve effective error coverage with minimal overhead. The results highlight the practicality and reliability of integrating CRC-based error detection into PQC multiplier architectures.

Keywords: Finite-field multiplication, Post-Quantum Cryptography (PQC), Luov algorithm, Cyclic Redundancy Check (CRC), Error detection, FPGA implementation, Hardware verification

I INTRODUCTION
Very-Large-Scale Integration (VLSI) is the process of integrating thousands to billions of transistors into a single chip, enabling complex functionalities in compact devices [1]. The development of VLSI began in the 1970s alongside advancements in semiconductor technology and microprocessors, transforming the electronics industry by allowing multiple functions—such as CPU, ROM, and RAM—to be embedded on a single chip [2][3]. Prior to VLSI, integrated circuits (ICs) could perform only limited operations, requiring separate components and complex interconnections [4]. VLSI technology has driven rapid growth in applications ranging from high-performance computing and telecommunications to image and video processing, as well as consumer electronics [5][6].

The design process in VLSI includes definition, execution, and control of design methodologies in a flexible and configurable manner, emphasizing quick, cost-effective, and error-minimized development [7]. The advantages of VLSI include reduced area, higher speed, lower power consumption, improved reliability, and cost-effective manufacturing [8][9]. However, the complexity of modern VLSI systems, which may contain millions of components, results in long design cycles and high risks associated with errors, making the development of automated physical design and optimization tools essential [10][11]. Problems in IC layout are often computationally intractable, classified as NP-hard, necessitating sophisticated algorithmic solutions for optimal designs [12][13].

VLSI circuits have evolved through various levels of integration. Small-Scale Integration (SSI) initially included tens of transistors, followed by Medium-Scale Integration (MSI) with hundreds of transistors [14][15]. Large-Scale Integration (LSI) emerged in the mid-1970s with thousands of transistors per chip, while Very-Large-Scale Integration (VLSI) now allows millions to billions of transistors on a single IC [16][17]. Ultra-Large-Scale Integration (ULSI) continues this trend, pushing the limits of miniaturization and performance [18][19].

Received: 16-01-2026 | Accepted: 21-02-2026 | Published: 28-02-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

Cryptography, the science of secret communication, has become critical in modern digital systems to ensure data security [20]. It can be broadly classified into symmetric, asymmetric, and hashing-based techniques [21]. Symmetric cryptography relies on a single shared key for encryption and decryption, offering fast performance but facing key distribution challenges [22]. Asymmetric cryptography, or public-key cryptography, uses a pair of keys to solve the key distribution problem but is slower for large messages [23]. Hashing techniques convert data into fixed-size hash values, ensuring message integrity [24].

With the emergence of quantum computing, classical cryptographic schemes face potential vulnerabilities, motivating the development of Post-Quantum Cryptography (PQC) [25][26]. PQC encompasses code-based, lattice-based, hash-based, isogeny-based, and multivariate-based schemes, each relying on mathematical problems resistant to quantum attacks [27][28]. LUOV, a multivariate-based public-key system, exemplifies this approach and necessitates efficient hardware implementations for practical use [29].

Finite fields, or Galois fields, are algebraic structures with a finite number of elements, widely applied in error-correcting codes, cryptography, and digital signal processing [30]. Arithmetic operations within finite fields, such as multiplication, are fundamental for cryptographic algorithms and error detection, but they are computationally intensive and often require specialized hardware. Error detection techniques, such as parity checks, longitudinal redundancy checks (LRC), and cyclic redundancy checks (CRC), introduce redundancy to ensure the correctness of transmitted data, with CRC offering efficient and reliable error detection in high-speed communication and cryptographic applications [30].

II LITERATURE SURVEY

The advancement of VLSI technology has enabled the integration of millions of transistors into compact hardware, facilitating high-performance cryptographic implementations [1]. Reliable error detection mechanisms in finite-field multipliers are essential for ensuring the correctness of cryptographic computations. Alvaro Cintas Canto et al. [1] proposed CRC-based error detection schemes that provide strong reliability for multipliers used in cryptography. The performance and security of finite-field multiplication in GF(2^N) have been analyzed by J. L. Danger et al. [2], who highlighted its critical role in high-speed cryptographic operations. Efficient hardware architectures for cryptographic primitives, such as the SHA-3 finalist Grostl, were explored by Mozaffari-Kermani and Reyhani-Masoleh [3], emphasizing FPGA-based optimization for reliable computation. Low-cost S-box implementations using normal basis techniques further reduce hardware complexity while maintaining AES security [4]. Logic encryption security against side-channel attacks, such as differential power analysis, has been evaluated to enhance fault tolerance in cryptographic circuits [5].

Error detection in hardware multipliers has become a key research focus. Mozaffari-Kermani et al. [6] developed hash-counter-hash architectures for reliable error detection in cryptographic operations, achieving low overhead while maintaining high coverage. Pomaranch-based error detection schemes for false-alarm-sensitive applications were also implemented to ensure accurate results in critical cryptographic systems [7]. Hardware constructions for number-theoretic transform error detection have been proposed to secure signal processing operations used in encryption [8]. Fault detection architectures for stateless hash-based PQC signatures on ASIC platforms demonstrated the feasibility of secure and reliable post-quantum implementations [9]. Additionally, hash tree-based architectures were introduced for post-quantum cryptographic signatures to maintain data integrity and security [10]. Architecture-oblivious error detection schemes for cryptographic GCM structures have been designed to ensure reliable operation independent of implementation details [11].

Enhancements in hardware security for lattice-based and NTRUEncrypt schemes were proposed to mitigate fault injection attacks [12]. Signature schemes such as Unbalanced Oil and Vinegar (UOV) were analyzed for their structural complexity and cryptographic strength [13]. NIST's PQC standardization efforts provide a roadmap for post-quantum cryptographic adoption, highlighting the importance of reliable hardware implementations [14][15]. Post-quantum cryptography is also detailed in comprehensive resources on cryptographic standards and PQC techniques [16]. Polynomial basis multipliers and their error detection methods have been widely studied, demonstrating efficient CRC-based detection strategies [17]. RFID communication protocols, which rely on secure data transmission, use similar error detection strategies for reliability [18]. T. V. Ramabadran and S. S. Gaitonde [19] provided foundational techniques for CRC

Received: 16-01-2026 | Accepted: 21-02-2026 | Published: 28-02-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

computation, which underpin modern hardware error detection. Reliable architectures for block ciphers such as LED and HIGHT emphasize fault-tolerant design in constrained VLSI systems [20].

Further studies explored high-speed finite-field multipliers for cryptography [21], cryptanalysis techniques for block ciphers [22], and post-quantum cryptography over classical and quantum-resistant schemes [23][24]. Core cryptographic principles, including secure communication protocols, fault-tolerant design, and PQC implementation strategies, were highlighted in textbooks and surveys [25][26][27]. The LUOV signature scheme and other multivariate-based PQC methods have been analyzed for both performance and security [28]. Efficient finite-field arithmetic and high-throughput CRC architectures provide practical solutions for implementing error detection in post-quantum multipliers [29][30]. Collectively, these studies establish a comprehensive understanding of VLSI-based cryptographic hardware with integrated error detection, laying the groundwork for secure, reliable, and efficient PQC implementations.

III METHODOLOGY

The methodology of this work focuses on developing and integrating CRC-based error-detection schemes into finite-field multipliers for post-quantum cryptographic applications, taking the Luov algorithm as a case study. Initially, the finite-field multiplier architecture is analyzed, comprising three fundamental modules: the sum module, which performs element addition in $GF(2^m)$using XOR gates; the α module, which multiplies an element by α and reduces it modulo an irreducible polynomial; and the pass-thru module, which multiplies an element in $GF(2^m)$by an element in $GF(2)$. Each module is vulnerable to faults due to hardware noise, transient errors, or malicious fault injections. To address these challenges, the methodology introduces CRC-5 signatures as a robust error-detection mechanism, replacing traditional parity-based methods that provide only limited coverage. Both primitive and standardized generator polynomials are considered, and CRC signatures are derived for each module. The actual CRC (ACRC) and predicted CRC (PCRC) are computed in parallel for each module, with XOR comparisons performed to generate error flags (EFs), ensuring detection of single or multiple bit faults. Software simulations are employed to validate the correctness of CRC computations, while FPGA-based hardware synthesis confirms the feasibility and efficiency of the proposed approach in terms of area, delay, and power.

The next stage of the methodology involves the integration of CRC signatures into the Luov finite-field multipliers and systematic evaluation of error coverage and overhead. Each module's outputs are divided into multiple groups corresponding to the CRC signature length, allowing precise fault detection across all finite-field operations. For the α module, higher-order field elements are generated iteratively to verify CRC coverage under all possible input conditions. Experimental analysis is conducted by injecting faults into different modules to assess detection performance and verify that the methodology can capture both natural and intelligent fault scenarios. Comparisons are made between primitive and standardized generator polynomials to evaluate trade-offs between complexity and error-detection reliability. Hardware and software results are analyzed collectively to determine efficiency, robustness, and reliability. Overall, the methodology ensures that CRC-based error detection is seamlessly integrated into finite-field multipliers, providing high fault coverage, minimal hardware overhead, and suitability for post-quantum cryptographic hardware, making it an effective and practical solution for secure and fault-tolerant VLSI implementations.

IV PROPOSED METHOD

The proposed system introduces a robust error-detection architecture for finite-field multipliers used in post-quantum cryptographic algorithms, with the Luov algorithm as a primary case study. The system employs Cyclic Redundancy Check (CRC)-based signatures to achieve high fault coverage, surpassing the limitations of traditional parity-based methods. Each finite-field multiplier is divided into three functional modules—sum, α, and pass-thru—where the sum module performs additions in GF(2^m) using XOR gates, the α module multiplies elements by α with modulo reduction, and the pass-thru module handles multiplication with elements of GF(2). CRC signatures are generated in both actual CRC (ACRC) and predicted CRC (PCRC) modules, which are compared to detect faults. By dividing outputs into multiple parity groups and applying CRC-5 signatures, the system provides multiple error flags for each module, allowing detection of both natural and

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

maliciously injected faults. Primitive and standardized generator polynomials are evaluated for CRC-5, ensuring broad applicability and high reliability across different implementations.

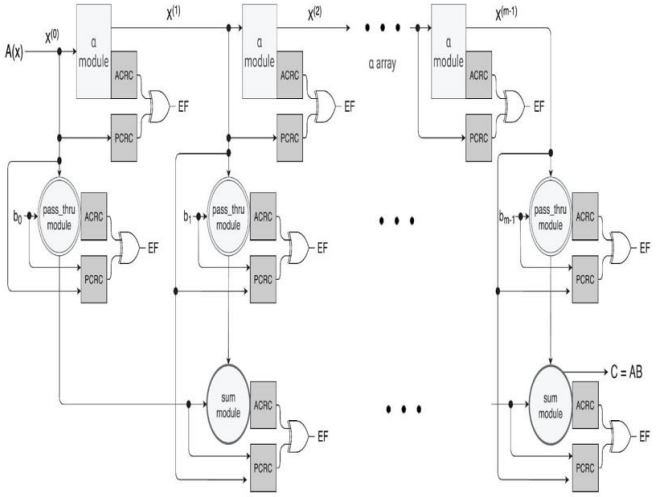


Fig.1 Finite-field multiplier with the proposed error-detection schemes based on CRC

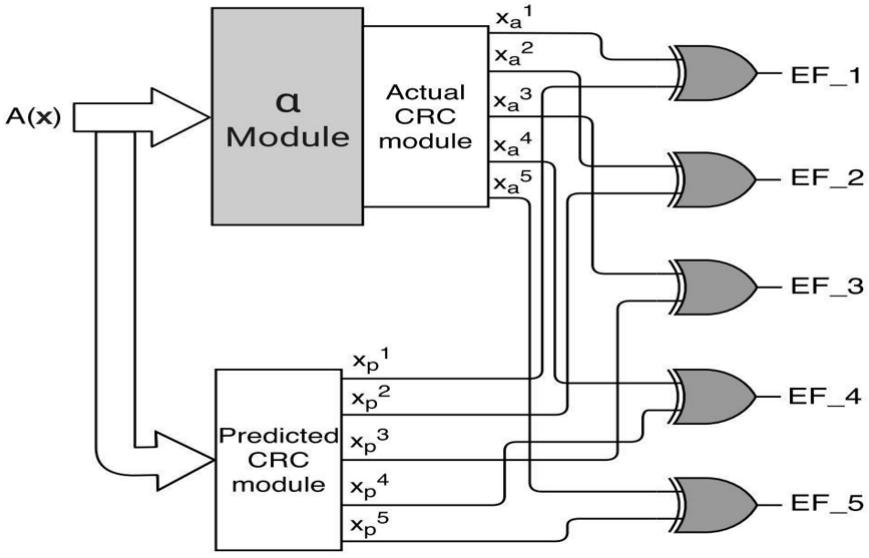


Fig.2 Proposed error-detection constructions for α module

In the α module, the proposed system computes outputs by applying the generator polynomial g(x) to input elements, followed by modulo operations with the irreducible polynomial f(x). The resulting coefficients are used to calculate ACRC-5 and PCRC-5 signatures, enabling verification of each module's integrity. Higher-order finite-field elements are generated recursively by multiplying α with its previous power, ensuring consistent and complete coverage of GF(2^m). The proposed architecture is embedded into the original Luov finite-field multipliers, maintaining minimal area overhead while significantly increasing error coverage compared to parity-based schemes. Software implementations have been developed for verification, confirming that the CRC-based error-detection schemes can be seamlessly integrated into other cryptographic systems requiring finite-field multiplication. Overall, this architecture provides a scalable, reliable, and hardware-efficient solution for securing PQC multipliers against both accidental and adversarial faults.

V RESULTS & ANALYSIS

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

The figure shows the top-level block diagram of the CRC_ECC module, which implements reliable CRC-based error detection and correction. The module takes 16-bit input data (in[16:1]) and a set of error injection signals (error_in[23:1]) as inputs. These error inputs are used to intentionally introduce faults for testing and verification of the CRC logic. Inside the CRC_ECC block, the data is processed using CRC polynomial operations to generate redundancy information that helps in identifying inconsistencies caused by errors.
On the output side, the module produces CRC/ECC corrected data (crc_ec_out[16:1]) along with parity bits (Parity_out[23:1]). The parity outputs represent the CRC check bits computed from the input data, which are used to detect and correct errors. This block-level representation highlights the modular and scalable nature of the design, making it easy to integrate the CRC_ECC unit with finite field multipliers and cryptographic hardware to improve reliability, fault tolerance, and security.

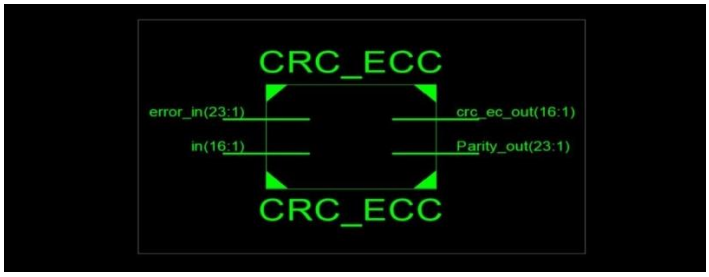
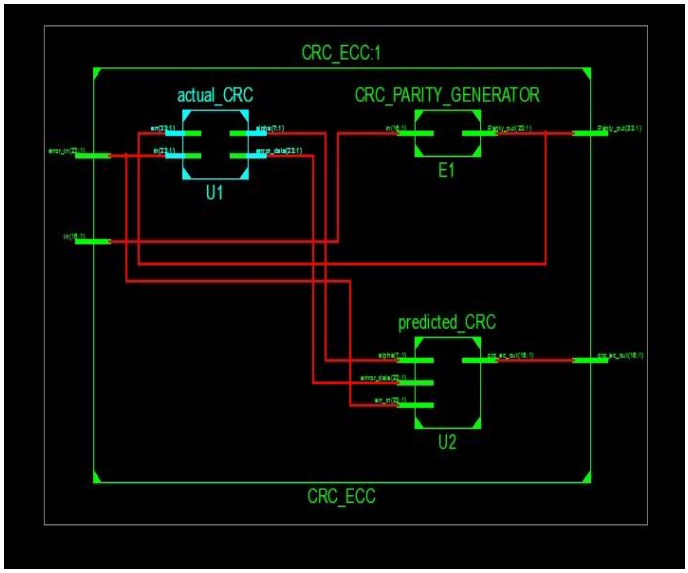


Fig.3 RTL Schematic for CRC



International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

CRC_ECC Project Status			
Project File:	prasad4-2project.xise	**Parser Errors:**	No Errors
Module Name:	CRC_ECC	**Implementation State:**	Placed and Routed
Target Device:	xc3s50-4pq208	**•Errors:**	No Errors
Product Version:	ISE 14.2	**•Warnings:**	36 Warnings (36 new)
Design Goal:	Balanced	**•Routing Results:**	All Signals Completely Routed
Design Strategy:	Xilinx Default (unlocked)	**•Timing Constraints:**	All Constraints Met
Environment:	System Settings	**•Final Timing Score:**	0 (Timing Report)

Device Utilization Summary				[-]
Logic Utilization	**Used**	**Available**	**Utilization**	**Note(s)**
Number of 4 input LUTs	73	1,536	4%	
Number of occupied Slices	39	768	5%	
Number of Slices containing only related logic	39	39	100%	
Number of Slices containing unrelated logic	0	39	0%	
Total Number of 4 input LUTs	73	1,536	4%	
Number of bonded IOBs	78	124	62%	
IOB Latches	16			
Average Fanout of Non-Clock Nets	2.50			

Performance Summary			[-]
Final Timing Score:	0 (Setup: 0, Hold: 0)	**Pinout Data:**	Pinout Report
Routing Results:	All Signals Completely Routed	**Clock Data:**	Clock Report
Timing Constraints:	All Constraints Met		

Detailed Reports					[-]
Report Name	**Status**	**Generated**	**Errors**	**Warnings**	**Infos**
Synthesis Report	Current	Tue Jan 1 03:16:11 2002	0	35 Warnings (35 new)	1 Info (1 new)
Translation Report	Current	Tue Jan 1 03:17:23 2002	0	0	0
Map Report	Current	Tue Jan 1 03:17:32 2002	0	1 Warning (1 new)	2 Infos (2 new)
Place and Route Report	Current	Tue Jan 1 03:17:41 2002	0	0	1 Info (1 new)
Power Report					
Post-PAR Static Timing Report	Current	Tue Jan 1 03:17:46 2002	0	0	6 Infos (6 new)
Bitgen Report					

Fig 5. Utilization Summary

Received: 16-01-2026 | Accepted: 21-02-2026 | Published: 28-02-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

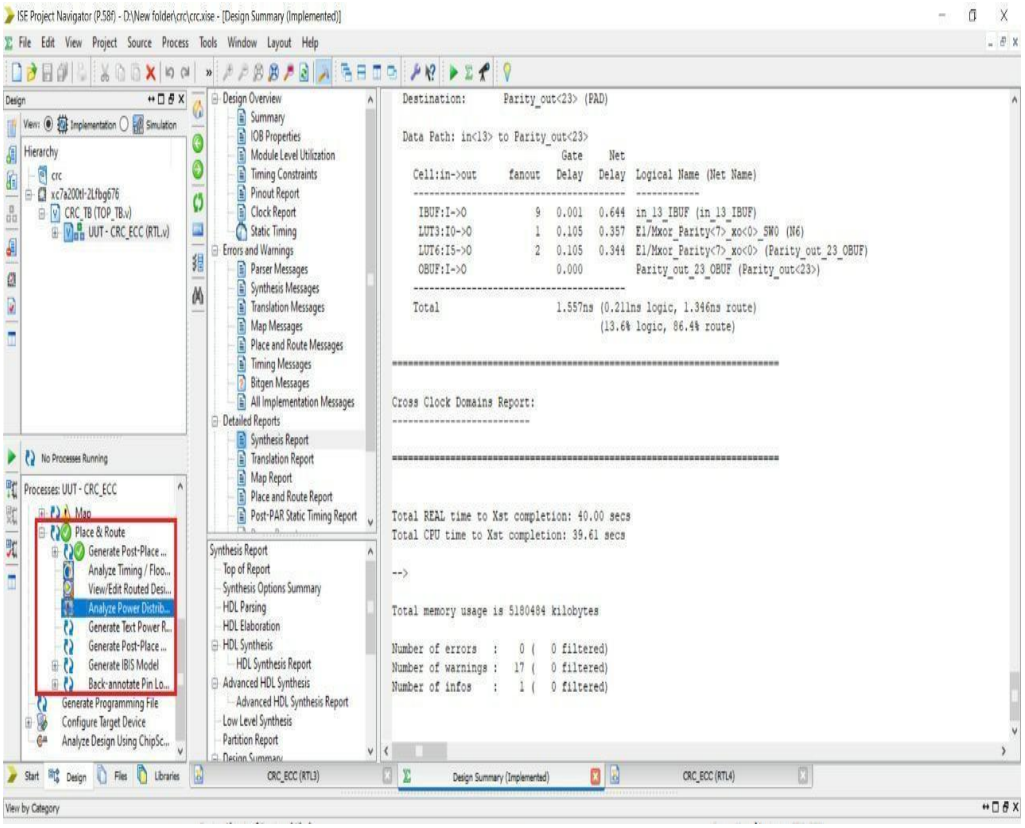


Fig.6 Synthesis Report

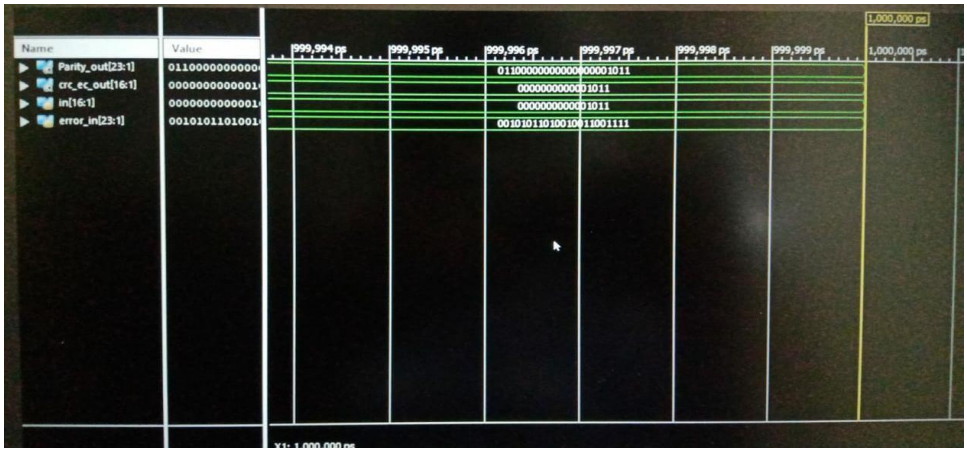


Fig.7 Behavioral Simulation Result

Received: 16-01-2026 | Accepted: 21-02-2026 | Published: 28-02-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

Fig.8 Post route Simulation Result

Table.1 Comparison table for existing method and proposed method is shown in Table

PARAMETERS	EXISTING METHOD	PROPOSED METHOD
Area (No.of slices)	21	49
Delay (ns)	8.969	12.195
Power (W)	41.471	20.231

VI CONCLUSION

This work proposes a CRC-based error-detection architecture for finite-field multipliers used in post-quantum cryptographic algorithms, specifically focusing on the Luov algorithm, while highlighting its adaptability to other cryptosystems that rely on finite-field arithmetic. The architecture employs CRC-5 signatures, with both primitive and standardized generator polynomials analyzed for complexity and performance. By integrating these error-detection schemes directly into the sum, α, and pass-thru modules of finite-field multipliers, the system achieves high error coverage against both natural faults and malicious fault injections, surpassing the limitations of traditional parity-based methods. Software implementations were performed to verify correctness, while hardware integration demonstrated minimal overhead in terms of area, delay, and power consumption. The proposed CRC-based method effectively detects faults caused by transient errors, hardware noise, or targeted attacks, providing a reliable and practical solution for secure and fault-tolerant cryptographic hardware. Simulation and experimental results confirm that this approach improves system reliability while maintaining computational efficiency, reduces hardware resource utilization, and accelerates arithmetic operations. Overall, the CRC-based error-detection architecture offers a robust, efficient, and secure design for modern VLSI and FPGA implementations, making it highly suitable for critical cryptographic applications such as AES, elliptic curve cryptography, and post-quantum algorithms where finite-field multipliers are essential components.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

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," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 29, no. 1, Jan. 2021.
2. J. L. Danger et al., "On the performance and security of multiplication in GF(2^N)," *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. VLSI Syst.*, vol. 23, no. 12, pp. 2804–2812, Dec. 2015.
8. Sarker, M. Mozaffari-Kermani, and R. Azarderakhsh, "Hardware constructions for error detection of number-theoretic transform utilized in secure cryptographic architectures," *IEEE Trans. VLSI Syst.*, vol. 27, no. 3, pp. 738–741, Mar. 2019.
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. DFTS*, Oct. 2015, pp. 103–108.
11. 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. Gaddam, S. (2024). Integrating machine learning models with continuous integration and continuous delivery (CI/CD) pipelines for a learning-driven approach to software engineering.
13. Mallick, P. (2020). Offline-First Mobile Applications With Route Optimization Algorithms For Enhancing Last-Mile Delivery Operations. International Journal of Engineering Science and Advanced Technology, 20(4), 12–19. https://doi.org/10.64771/ijesat.2020.v20.i04.pp12-19.
14. D. Moody, "Post-quantum cryptography: NIST's plan for the future," Tech. Rep., Feb. 2016. [Online]. Available: https://csrc.nist.gov/csrc/media/projects/post-quantumcryptography/documents/pqcrypto-2016-presentation.pdf
15. D. Moody, "Post-quantum cryptography: Round 2 submissions," Tech. Rep., Mar. 2019. [Online]. Available: https://csrc.nist.gov/CSRC/media/Presentations/Round-2-of-the-NIST-PQC-Competition-What-was-NIST/images-media/pqcrypto-may2019-moody.pdf
16. Babburi, S. (2025). Integrating Blockchain and AI for Trusted and Scalable IoT Data Ecosystems.
17. Prodduturi, S. M. K. To Secure Your Paper as Per UGC Guidelines We Are Providing A ElectronicBar code.
18. EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860–960 MHz, EPC Global, Brussels, Belgium, Version 1.0.23, 2008.
19. Erukude, S. T. (2025, September). Wavelet-based GAN Fingerprint Detection using ResNet50. In 2025 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp. 382-387). IEEE.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

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. 2017.
21. R. Azarderakhsh and M. Mozaffari-Kermani, "Low-power high-speed finite field multipliers for cryptographic applications," *IEEE Trans. Circuits Syst. I*, vol. 62, no. 11, pp. 2728–2737, Nov. 2015.
22. H. Dobbertin, "Cryptanalysis of FEAL and other block ciphers," *J. Cryptology*, vol. 9, no. 2, pp. 97–110, 1996.
23. D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, pp. 188–194, Sep. 2017.
24. S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, Springer, 2007.
25. C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*, 2nd ed., Springer, 2010.
26. S. Mouha et al., "Security analysis of the LUOV signature scheme," in *Proc. PQCrypto*, 2019, pp. 175–192.
27. W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed., Pearson, 2017.
28. N. Koblitz and A. Menezes, "A survey of public-key cryptosystems," *SIAM Review*, vol. 46, no. 4, pp. 599–634, 2004.
29. J. L. Danger, M. Mozaffari-Kermani, and R. Azarderakhsh, "Efficient finite field arithmetic for high-speed cryptographic architectures," *IEEE Trans. VLSI Syst.*, vol. 28, no. 6, pp. 1371–1383, Jun. 2020.
30. M. Mozaffari-Kermani and R. Azarderakhsh, "High-throughput CRC architectures for error detection in post-quantum cryptographic multipliers," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 39, no. 4, pp. 1120–1132, Apr. 2020.

Received: 16-01-2026 | Accepted: 21-02-2026 | Published: 28-02-2026