



Balanced Resource-Reuse Karatsuba Multiplier Architecture for 256-Bit ECC on FPGA

R. RajaRaja¹ · V. R. Venkatasubramani² · A. Babu Karuppiiah³ · S. Rajaram²

Received: 18 December 2025 / Revised: 4 August 2026 / Accepted: 5 August 2026

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2026

Abstract

Elliptic curve cryptography (ECC) over binary finite fields relies heavily on polynomial multiplication, making the efficiency of the underlying multiplier architecture a critical factor in cryptographic hardware design [23]. Among various approaches, Karatsuba multiplication is widely adopted due to its reduced arithmetic complexity; however, aggressive parallelism and improper resource reuse often lead to excessive power consumption and thermal infeasibility on FPGA platforms [11, 26]. This paper presents a comprehensive architectural exploration of seven 256-bit Karatsuba-based binary polynomial multiplier architectures over Galois Field (GF) (2^{256}), each employing a different resource-reuse strategy ranging from fully parallel to fully sequential implementations. All architectures are implemented on a Xilinx Artix-7 FPGA using identical synthesis and power estimation settings to ensure a fair comparison in terms of area, latency, power consumption, and junction temperature. The study reveals that fully parallel Karatsuba architectures, although fast, are thermally impractical due to excessive switching activity, while fully sequential designs suffer from high latency. Based on these insights, a balanced resource-reuse architecture is identified, which selectively reuses multiplier blocks from 16-bit to 128-bit levels while retaining parallelism at lower levels. Compared to the fully sequential Karatsuba architecture, the proposed balanced design reduces computation latency by more than $26 \times$ (121 cycles vs. 3280 cycles) while maintaining thermally safe operation (73.0 °C) and consuming only 18% higher power (25.66 W vs. 21.77 W). This balanced trade-off makes the proposed architecture particularly suitable for FPGA-based ECC accelerators requiring both performance and energy efficiency.

Keywords Elliptic curve cryptography · Binary polynomial multiplication · Karatsuba multiplier · Resource reuse architecture · FPGA implementation · Power and thermal analysis

1 Introduction

The rapid expansion of secure digital communication in embedded and resource-constrained systems has intensified the demand for efficient cryptographic hardware accelerators. Applications such as wireless sensor networks, Internet of Things (IoT) devices, and secure edge computing require cryptographic solutions that not only provide strong security but also operate within strict constraints on area, power consumption, and thermal dissipation. In this context, Elliptic Curve Cryptography (ECC) has emerged as a preferred public-key cryptographic technique due to its ability to achieve equivalent security with significantly shorter key lengths compared to traditional schemes such as RSA [22, 23, 27]. The practical performance of ECC hardware implementations is largely determined by the efficiency of finite-field arithmetic, particularly field multiplication, which dominates the computational complexity of point addition and point multiplication operations. For ECC implementations over binary fields, polynomial basis representation is widely adopted because of its suitability for hardware realization. In such systems, the design of an efficient binary polynomial multiplier directly impacts not only area and latency but also dynamic power consumption and thermal behavior of the cryptographic processor. Among the various multiplication algorithms proposed for large-degree polynomial arithmetic, the Karatsuba algorithm has attracted considerable attention due to its reduced arithmetic complexity. By recursively decomposing operands into smaller sub-operands, Karatsuba multiplication reduces the number of required partial multiplications from quadratic to sub-quadratic complexity. As a result, Karatsuba-based multipliers are extensively used in FPGA-based ECC accelerators to improve performance and scalability for large operand sizes such as 256 bits [11, 13, 26]. However, the recursive nature of the Karatsuba algorithm introduces important architectural design challenges. Fully parallel implementations, in which all recursive sub-multipliers are instantiated simultaneously, can achieve very low latency but at the cost of substantial hardware resources and excessive switching activity. On FPGA platforms, this aggressive parallelism often leads to high dynamic power consumption and unrealistic thermal conditions, making such designs impractical for real deployments. Conversely, fully resource-reused or sequential Karatsuba architectures significantly reduce area and switching activity by time-multiplexing a small base multiplier across recursion levels, but they incur large latency due to serialized computation [26, 35].

Despite the extensive use of Karatsuba multiplication in ECC hardware, most existing works focus on optimizing a single architectural variant or emphasize improvements in either area or speed alone. A systematic exploration of the broader Karatsuba architectural design space—ranging from fully parallel to fully sequential implementations—under a unified evaluation framework is still lacking [13, 25, 37]. Moreover, thermal feasibility, which has become increasingly critical with rising FPGA integration densities, is rarely considered as a primary design constraint in multiplier architecture selection. Motivated by these observations, this paper presents a comprehensive architectural study of seven 256-bit Karatsuba-based binary polynomial multiplier designs for ECC over $GF(2^{256})$. Each architecture employs a distinct resource-reuse strategy, varying the degree of parallelism and time multiplexing across recursion levels. All architectures are implemented on the same Xilinx Artix-7 FPGA

To further improve the realism of power estimation, an additional analysis was performed by modifying the switching activity parameters in Vivado. In the default vectorless mode, a uniform toggle rate of 12.5 is assumed across all nodes, which can lead to overestimation of dynamic power, particularly in architectures with large parallel combinational logic.

In the refined analysis, the toggle rate was reduced to 0.5 to better approximate realistic switching activity in FPGA datapath circuits. Additionally, activity scaling was applied to logic elements, with LUTs and registers assigned appropriate switching activity, while primary outputs were assigned zero activity. These parameters were applied uniformly across all architectures to ensure fair comparison.

The resulting power values, presented in Table 5, fall within the milliwatt range and represent a more practical estimation of power consumption for FPGA-based implementations. Notably, the proposed balanced architecture (Architecture-7) achieves a power consumption of 659 mW. It achieves near-minimum power while significantly reducing latency and providing an efficient balance between power, latency, and area, making the proposed architecture better than other architectures.

This additional analysis complements the default estimation and provides improved insight into the power characteristics of the evaluated architectures under realistic switching conditions.

7 Conclusion

Among the evaluated Karatsuba architectures, the proposed balanced resource-reuse design (Architecture-7) achieves the most favorable trade-off between performance and energy efficiency. While fully parallel architectures achieve minimal latency at the cost of extreme switching activity and thermal infeasibility, and fully sequential architectures minimize power at the expense of prohibitive latency, the proposed design bridges this gap. Specifically, it reduces latency by over $26\times$ compared to the fully sequential design while operating within safe thermal limits and incurring only a marginal increase in power consumption. These results demonstrate that selective reuse at switching-dominant recursion levels is a key architectural principle for practical FPGA-based ECC multipliers. This paper presented a systematic architectural exploration of seven 256-bit Karatsuba-based binary polynomial multiplier designs for Elliptic Curve Cryptography over $GF(2^{256})$, with particular emphasis on area efficiency, power consumption, latency, and thermal feasibility on FPGA platforms. Unlike prior works that focus on optimizing a single architectural variant, this study evaluated a wide spectrum of resource-reuse strategies under a unified synthesis-level evaluation framework. The results demonstrate that extreme architectural choices are impractical for real FPGA deployments. Fully parallel Karatsuba implementations achieve minimal latency but suffer from excessive switching activity, leading to prohibitively high-power consumption and thermally unsafe operation. Conversely, fully reused sequential designs minimize power dissipation but incur very high latency, limiting their applicability in performance-critical ECC applications. Intermediate reuse strategies partially mitigate these issues but often fail to simultaneously satisfy all

design constraints. Based on the comparative analysis, a balanced Karatsuba architecture employing selective resource reuse from the 16-bit to the 128-bit recursion levels was identified as the practically deployable architecture among the evaluated designs. By explicitly controlling the number of simultaneously active 2-bit multipliers at higher recursion levels while retaining parallelism at lower levels, the proposed architecture achieves a superior trade-off among logic utilization, latency, power consumption, and thermal behavior. Synthesis-level results confirm that this balanced design operates within safe thermal limits while delivering significantly improved performance compared to fully sequential approaches.

Although the reported power and thermal values are based on synthesis-level estimates, the observed trends clearly highlight the effectiveness of selective reuse as a key design principle for power- and thermally-efficient FPGA-based ECC multipliers. The presented analysis provides practical guidance for hardware designers in selecting appropriate Karatsuba architectures based on application-specific performance and energy constraints. Future work will focus on extending the proposed architecture to post-implementation power analysis and on-board FPGA measurements to further validate the observed trends. Additional research directions include pipelining and clock-gating techniques to further reduce dynamic power, adaptation of the architecture to different field sizes and irreducible polynomials, and integration of the multiplier into a complete ECC processor to evaluate system-level performance.

7.1 Future Work

While the present study relies on synthesis-level power estimation for consistent architectural comparison, post-implementation measurements on physical FPGA hardware will be considered in future work to further validate the observed trends. Integrating the proposed balanced Karatsuba multiplier into a complete ECC processor for system-level validation will also be the direction for the future work.

Funding No funding was received.

Data availability All data generated or analyzed during this study are included in this article. Additional data supporting the findings of this work are available from the corresponding author upon reasonable request.

Declarations

Competing interests The authors declare that there are no conflicts of interest regarding the publication of this paper.

Declaration of generative AI and AI-Assisted Technologies in the Manuscript Preparation Process During the preparation of this work, the authors used ChatGPT (OpenAI, GPT-4 model) to assist in improving the clarity, language, and structure of the manuscript text. After using this tool, the authors thoroughly reviewed, verified, and edited all content to ensure that it accurately reflects their own analysis and original contributions. The authors take full responsibility for the content of this publication.

References

1. R. Abu-Salma, M.A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, M. Smith, Obstacles to the adoption of secure communication tools, in *Proceedings of the IEEE Symposium Security and Privacy (SP)* (2017), pp. 137–153. <https://doi.org/10.1109/SP.2017.65>
2. V. Anbumani, S. Padmapriya, R. Rajaraja, N. Vikram, S. Ranjith, Efficient fault detection methods in printed circuit boards using machine learning techniques, in *Proceedings of the 15th International Conference Computing, Communication and Networking Technologies* (2024)
3. D.K.S.V. Anbumani, N. Vikram, R. Rajaraja, G.P. Sanjeev, M.J. Varunesh, Area-efficient VLSI architecture for Advanced Encryption Standard. in *Proceedings of the 15th International Conference Computing, Communication and Networking Technologies* (2024)
4. A. Arunachalamani, V.R. Venkatasubramani, V.V. Thyagarajan, S. Rajaram, High-radix design for Montgomery multiplier on FPGA platform, in *Proceedings of the International Conference Recent Advances in Electrical, Electronics and Communication Engineering* (2023)
5. S. Banerjee, A. Patil, ECC based encryption algorithm for lightweight cryptography. *Adv. Intell. Syst. Comput.* **921**, 600–609 (2020)
6. A. Birgani, M. Timarchi, S. Khalid, Area–time-efficient scalable schoolbook polynomial multiplier for lattice-based cryptography. *IEEE Trans. Circuits Syst. II* **69**(12), 4957–4961 (2022). <https://doi.org/10.1109/TCSII.2022.3184721>
7. A. Dhanush, V. Vijayakumar, Solvability and optimal feedback control results for higher order fractional differential systems. *J. Optim. Theory Appl.* **208**, Art. no. 31 (2026). <https://doi.org/10.1007/s10957-025-02862-7>
8. A. Dhanush, V. Vijayakumar, Time optimal control results for Hilfer fractional neutral stochastic differential equations. *Complex Anal. Oper. Theory*, **19**, Art. no. 120 (2025). <https://doi.org/10.1007/s11785-025-01748-w>
9. A. Dhanush, V. Vijayakumar, Discussion on the approximate controllability results for neutral fractional differential systems with state-dependent delay. *Asian J. Control* **28**(1), 486–496 (2026). <https://doi.org/10.1002/asjc.3793>
10. M. Esmaeildoust, D. Schinianakis, H. Javashi, T. Stouraitis, K. Navi, Efficient RNS implementation of elliptic curve point multiplication over GF(p). *IEEE Trans. VLSI Syst.* **21**(8), 1545–1549 (2013). <https://doi.org/10.1109/TVLSI.2012.2226523>
11. H. Fan, J.-G. Sun, M. Gu, K.-Y. Lam, Overlap-free Karatsuba-Ofman polynomial multiplication algorithms. *IET Inf. Security* **4**(1), 8–14 (2010). <https://doi.org/10.1049/iet-ifs.2009.0064>
12. R. Gowda, S. Shaila, K.R. Venugopal, Elliptic curve crypto processor on FPGA using Montgomery multiplication over GF(2^m), in *Proceedings of the International Conference Inventive Communication and Information Systems* (2018), pp. 367–372. <https://doi.org/10.1109/ICIS.2018.8716345>
13. M. Heidarpur, M. Mirhassani, An efficient and high-speed overlap-free Karatsuba-based finite-field multiplier for FPGA implementation. *IEEE Trans. VLSI Syst.* **29**(4), 667–676 (2021). <https://doi.org/10.1109/TVLSI.2020.3047514>
14. S. Hu, J. Lin, Q. Tang, Y. Liu, AC-PM: an area-efficient and configurable polynomial multiplier for lattice-based cryptography. *IEEE Trans. Circuits Syst. I* **70**(10), 4060–4072 (2023). <https://doi.org/10.1109/TCSI.2023.3289035>
15. M. Kalaiarasi, V.R. Venkatasubramani, M.S.K. Manikandan, S. Rajaram, High-performance HITA-based binary Edwards curve crypto processor for FPGA platforms. *J. Parallel Distrib. Comput.* **178**, 56–68 (2023)
16. A.B. Karuppiiah, R. Rajaraja, Introduction to modern FET technologies, in *Field Effect Transistors*. (2025), pp.45–61
17. A.B. Karuppiiah, V. Nanjappan, R. Rajaraja, S.V. Priyan, Neuro inspired deep learning based secure and energy efficient routing with autonomous intrusion prevention in wireless sensor networks. *Eng. Appl. Artif. Intell.* **162**, Art. no. 112783 (2025)
18. A.B. Karuppiiah, R. Rajaraja, P. Suveetha Dhanaselvam, An ultra-lightweight hardware efficient cryptography algorithm for wireless sensor networks. *Lib. Progress Int.* **44**(3), 20933–20943 (2024).
19. A.B. Karuppiiah, R. Rajaraja, R.M. Resma, S. Susithra, N. Pradeepika, G. Gopika, Resource analysis of lightweight cryptography algorithms for compact devices, in *Proceedings of the International Conference Smart Systems for Electrical, Electronics, Communication and Computer Engineering (ICSSECC)* (2024), pp. 579–584.

20. A.B. Karuppiiah, R. Rajaraja, An enhanced and secured wireless environment using swept frequency capacitive sensing. *Asian J. Inf. Technol.* **15**(18), 3545–3550 (2017)
21. Z.U.A. Khan, M. Benaissa, High-speed and low-latency ECC processor implementation over $GF(2^m)$ on FPGA. *IEEE Trans. VLSI Syst.* **25**(1), 165–176 (2017). <https://doi.org/10.1109/TVLSI.2016.2597310>
22. N. Koblitz, Elliptic curve cryptosystems. *Math. Comput.* **48**(177), 203–209 (1987). <https://doi.org/10.1090/S0025-5718-1987-0866109-5>
23. C.A. Lara-Niño, A. Díaz-Pérez, M. Morales-Sandoval, Elliptic curve lightweight cryptography: a survey. *IEEE Access* **6**, 72514–72550 (2018). <https://doi.org/10.1109/ACCESS.2018.2877298>
24. L. Li, S. Li, High-performance pipelined architecture of elliptic curve scalar multiplication over $GF(2^m)$. *IEEE Trans. VLSI Syst.* **20**(8), 1392–1400 (2012). <https://doi.org/10.1109/TVLSI.2011.2159250>
25. Y. Li, Y. Zhang, W. He, Fast hybrid Karatsuba multiplier for type II pentanomials. *IEEE Trans. VLSI Syst.* **28**(11), 2459–2463 (2020). <https://doi.org/10.1109/TVLSI.2020.3013200>
26. P.K. Meher, Efficient FPGA implementation of low-complexity systolic Karatsuba multiplier over $GF(2^m)$ based on NIST polynomials. *IEEE Trans. Circuits Syst. I* **64**(5), 1243–1256 (2017). <https://doi.org/10.1109/TCSI.2017.2659661>
27. V.S. Miller, Use of elliptic curves in cryptography, in *Advances in Cryptology—CRYPTO '85*, LNCS 218 (1986), pp. 417–426. https://doi.org/10.1007/3-540-39799-X_31
28. D. Pamula, A. Tisserand, Fast and secure finite field multipliers, in *Proceedings of the Euromicro Conference Digital System Design (DSD)* (2015). <https://doi.org/10.1109/DSD.2015.11>
29. A. Percey, *Advantages of the Virtex-5 FPGA 6-Input LUT Architecture*, Xilinx White Paper WP284, 2007.
30. A.D. Piccoli, A. Visconti, O.G. Rizzo, Polynomial multiplication over binary finite fields: new upper bounds. *J. Cryptogr. Eng.* **10**, 197–210 (2020). <https://doi.org/10.1007/s13389-019-00216-7>
31. R. Rajaraja, D. Pavithra, Implementation of hardware efficient lightweight encryption method, in *Proceedings of the International Conference Communication and Signal Processing (ICCSP)* (2013), pp. 191–195
32. R. Rajaraja, A.B. Karuppiiah, A reliable algorithm with increased accuracy for drone detection. *Periodico di Mineralogia* **91**(4), 426–435 (2022)
33. R. RajaRaja, V.R. Venkatasubramani, A. Babu Karuppiiah, S. Rajaram, A power-efficient 256-bit overlap-free karatsuba multiplier architecture for ECC on FPGA platforms. *IETE J. Res.* (2026), pp. 1–13. <https://doi.org/10.1080/03772063.2026.2699925>
34. S. Raza, L. Seitz, D. Sitenkov, G. Selander, S3K: scalable security with symmetric keys—DTLS key establishment for the Internet of Things. *IEEE Trans. Autom. Sci. Eng.* **13**(3), 1270–1280 (2016). <https://doi.org/10.1109/TASE.2016.2527729>
35. A. Reyhani-Masoleh, M.A. Hasan, Low complexity bit-parallel architectures for polynomial basis multiplication over $GF(2^m)$. *IEEE Trans. Comput.* **53**(8), 945–959 (2004). <https://doi.org/10.1109/TC.2004.31>
36. A. Sanjana, V.R. Venkatasubramani, S. Rajaram, M. Kalaiarasi, An improved octet Itoh–Tsujii algorithm for FPGA platforms, in *Proceedings of the International Conference Energy, Materials and Communication Engineering* (2023).
37. S. Thirumoorthi, M. Heidarpur, An optimized M-term Karatsuba-like binary polynomial multiplier for finite field arithmetic. *IEEE Trans. VLSI Syst.* **30**(4), 563–574 (2022). <https://doi.org/10.1109/TVLSI.2021.3135804>
38. M. Thirumoorthi, A.J. Leigh, M. Heidarpur, M.A.S. Khalid, M. Mirhassani, Novel formulations of M-term overlap-free Karatsuba binary polynomial multipliers and their hardware implementations. *IEEE Trans. VLSI Syst.* (2023). <https://doi.org/10.1109/TVLSI.2023.3299508>
39. J.A. Vidhya, V.R. Venkatasubramani, S. Rajaram, V.V. Thyagarajan, An FPGA-optimized parallel processor architecture for Huff curves with reduced clock cycles, in *Proceedings of the International Conference Interdisciplinary Approaches in Engineering and Technology*, 2025.
40. J.A. Vidhya, V.R. Venkatasubramani, S. Rajaram, Low-latency binary Edwards curve crypto processor for FPGA platforms, in *Proceedings of the International Conference Applications and Techniques in Information Security* (2024)
41. J.A. Vidhya, V.R. Venkatasubramani, S. Rajaram, V.V. Thyagarajan, Low latency binary Edwards curve cryptosystem, in *Applications and Techniques in Information Security, 14th International Conference* (2024)

42. C. Wang, Y. Zhang, Z. Li, X. Liu, High-throughput Toom–Cook-4 polynomial multiplier for lattice-based cryptography. *IEEE Trans. Circuits Syst. I* **71**(1), 359–372 (2024). <https://doi.org/10.1109/TCSI.2023.3312456>
43. H. Wu, M.A. Hasan, I.F. Blake, S. Gao, Finite field multiplier using redundant representation. *IEEE Trans. Comput.* **51**(11), 1306–1316 (2002). <https://doi.org/10.1109/TC.2002.1047755>
44. K. Yuvashri, J. Dalfiah, A.B. Karuppiyah, R. Rajaraja, Efficient algorithm for accurate detection of Sybil attack in a wireless sensor network. *Int. J. Appl. Eng. Res.* **10**(55), 1429–1432 (2015)
45. M. Zeghid, H.Y. Ahmed, A. Chehri, A. Sghaier, Speed/area-efficient ECC processor implementation over GF(2^m) on FPGA via novel algorithm-architecture co-design. *IEEE Trans. Very Large Scale Integr. VLSI Syst.* **31**(8), 1192–1203 (2023)
46. X. Zhang, J. Long, Z. Wang, H. Cheng, Lossless and reversible data hiding in encrypted images with public-key cryptography. *IEEE Trans. Circuits Syst. Video Technol.* **26**(9), 1622–1631 (2016). <https://doi.org/10.1109/TCSVT.2015.2478071>
47. J. Zhang, Z. Chen, M. Ma, R. Jiang, A. Wang, W. Wang, H. Dang, High-performance elliptic curve scalar multiplication architecture based on interleaved mechanism. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **33**(3), 757–770 (2025). <https://doi.org/10.1109/TVLSI.2024.3486312>
48. D. Zoni, A. Galimberti, W. Fornaciari, Flexible and scalable FPGA-oriented design of multipliers for large binary polynomials. *IEEE Access* **8**, 75809–75821 (2020). <https://doi.org/10.1109/ACCESS.2020.2989423>

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

Authors and Affiliations

R. RajaRaja¹ · V. R. Venkatasubramani² · A. Babu Karuppiyah³ · S. Rajaram²

✉ R. RajaRaja
birneraja@gmail.com

V. R. Venkatasubramani
venthiru@tce.edu

A. Babu Karuppiyah
babkarofficial@gmail.com

S. Rajaram
rajaram_siva@tce.edu

¹ Department of ECE, PSG Institute of Technology and Applied Research, Coimbatore, India

² Department of ECE, Thiagarajar College of Engineering, Madurai, India

³ Department of ECE, Sri Eshwar College of Engineering, Coimbatore, India