

A Power-Efficient 256-bit Overlap-Free Karatsuba Multiplier Architecture for ECC on FPGA Platforms

R. RajaRaja¹, V. R. Venkatasubramani², A. Babu Karuppiyah³ and S. Rajaram²

¹Department of ECE, PSG Institute of Technology and Applied Research, Coimbatore, India; ²Department of ECE, Thiagarajar College of Engineering, Madurai, India; ³Department of ECE, Sri Eshwar College of Engineering, Coimbatore, India

ABSTRACT

Elliptic Curve Cryptography (ECC) has emerged as a preferred security mechanism for resource-constrained Internet-of-Things (IoT) platforms due to its high security-to-key-size ratio. In hardware implementations of ECC over binary extension fields $GF(2^m)$, finite-field polynomial multiplication constitutes the most power-intensive operation. This work presents a power-efficient 256-bit overlap-free Karatsuba multiplier architecture implemented over $GF(2^m)$ and evaluated on the Xilinx Virtex-7 (xc7vx690tffg1761-2) FPGA platform. Binary extension fields are specifically chosen for their carry-free XOR-based arithmetic, which reduces logic depth and switching activity – advantages particularly suited to low-power FPGA implementations.

Two distinct architectural strategies are investigated: a fully instantiated hierarchical design and an iterative, resource-shared design. While the instantiated architecture achieves minimal latency through parallel computation, it incurs excessive switching activity and power dissipation. In contrast, the proposed iterative architecture employs a Finite State Machine (FSM) to enable controlled hardware reuse, thereby significantly reducing switching activity.

Post-synthesis analysis using Xilinx Vivado 2014.2 demonstrates that the iterative architecture achieves a reduction of approximately 89.5% in estimated dynamic power (from 590.37 W to 62.00 W) and 88.9% in total on-chip power (from 599.658 W to 66.325 W), at the cost of a 90.1% increase in LUT utilization (from 16,429 to 31,223). An analytical power model based on Karatsuba complexity is presented, confirming that dynamic power scales with exponent $\beta \approx 1.58$ (instantiated) and $\beta \approx 1.54$ (iterative), both closely consistent with the theoretical Karatsuba complexity ($\log_2 3 \approx 1.585$). The relevance of binary polynomial multiplication in emerging Post-Quantum Cryptography (PQC) schemes highlights the broader applicability of the proposed architecture.

KEYWORDS

ECC; binary polynomial multiplication; Karatsuba multiplier; Overlap-Free Karatsuba Algorithm (OKA); FPGA implementation; cryptographic hardware optimization

1. INTRODUCTION

The rapid growth of Internet-of-Things (IoT) devices and embedded systems has intensified the demand for secure and energy-efficient cryptographic solutions [1]. Public-key cryptography plays a fundamental role in ensuring data confidentiality, integrity, and authentication in such environments [2]. Among various approaches, Elliptic Curve Cryptography (ECC) has gained significant attention due to its ability to provide equivalent security with smaller key sizes compared to traditional algorithms such as RSA [3], thereby reducing computational and energy overheads [4].

At the hardware level, the efficiency of ECC implementations is largely determined by finite-field arithmetic operations, realized over either prime fields $GF(p)$ or binary extension fields $GF(2^m)$. Works such as [5,6] have explored high-performance modular multipliers over $GF(p)$ for ECC applications. While prime field

arithmetic is widely adopted in software implementations, binary fields $GF(2^m)$ offer distinct advantages for hardware realization. In $GF(2^m)$, addition is performed using bitwise XOR operations without carry propagation, significantly reducing logic complexity, critical path delay, and switching activity in FPGA-based architectures [7,8]. These characteristics make binary fields particularly suitable for low-power cryptographic hardware [9,10].

In addition to classical ECC applications, polynomial multiplication over $GF(2^m)$ has gained renewed importance in emerging Post-Quantum Cryptography (PQC) schemes, such as code-based and lattice-based cryptosystems, where large-degree polynomial arithmetic forms the computational backbone [11–15]. Earlier works [16–19] have also explored Vedic and Montgomery multiplier architectures for FPGA-based ECC implementations, providing complementary perspectives on hard-

ware design strategies. Recent works [20,21] further highlight the importance of efficient modular multipliers for PQC-based digital signature schemes.

The choice of finite field has significant implications for hardware design. Prime field $GF(p)$ arithmetic dominates software implementations and current ECC standards such as NIST P-256, due to compatibility with general-purpose processors and widespread library support [5,6]. However, $GF(p)$ operations require modular reduction involving carry propagation through multi-precision adder chains, increasing critical path delay and switching activity in FPGA implementations. In contrast, binary extension field $GF(2^m)$ arithmetic is inherently XOR-based – addition requires no carry propagation, and multiplication decomposes into bitwise polynomial operations that map efficiently onto FPGA Look-Up Tables (LUTs) [22]. This structural simplicity results in reduced logic depth, lower routing complexity, and diminished switching activity [23], making $GF(2^m)$ particularly advantageous for low-power FPGA-based cryptographic accelerators [7,8]. While $GF(p)$ offers performance advantages on high-end platforms, $GF(2^m)$ remains the preferred choice for energy-constrained implementations on devices such as the Xilinx Virtex-7 FPGA targeted in this work.

Among various multiplication algorithms, the Karatsuba–Ofman algorithm reduces computational complexity to $O(n^{1.585})$ compared to the conventional $O(n^2)$ approach. However, its hardware realization introduces challenges such as increased routing complexity, overlapping partial products, and elevated switching activity. Overlap-free Karatsuba architectures address these issues by eliminating redundant computations and isolating non-overlapping bit regions [8], leading to reduced logic depth and improved power efficiency.

Despite these advancements, existing FPGA-based Karatsuba implementations predominantly focus on improving speed or reducing area, often overlooking dynamic power consumption. A systematic evaluation of architectural trade-offs, particularly for 256-bit operands relevant to modern ECC standards, remains limited in the literature. This work addresses that gap by presenting a comparative power analysis of two 256-bit overlap-free Karatsuba architectures on the Virtex-7 platform.

The main contributions of this work are:

- Design and implementation of a scalable 256-bit overlap-free Karatsuba multiplier over $GF(2^m)$.

- Comparative analysis of fully parallel and iterative resource-shared architectures on Xilinx Virtex-7 FPGA.
- Quantitative evaluation of power and area trade-offs (LUTs, FFs, dynamic power, junction temperature) using post-synthesis estimation in Xilinx Vivado 2014.2.
- Development of an analytical power model with curve-fitting validation against Karatsuba complexity theory.
- Contextualisation of $GF(2^m)$ multiplier design within the broader landscape of $GF(p)$ and PQC multiplier architectures [5,6,20,21].

2. DESIGN MOTIVATION AND OPTIMIZATION NEED

2.1 Limitations of Existing Karatsuba Architectures

A survey of existing FPGA-based Karatsuba multiplier implementations reveals several limitations. Fully parallel or instantiated architectures are commonly adopted to achieve high throughput; however, these designs involve extensive duplication of sub-modules, leading to large switching activity across the FPGA fabric. This results in increased dynamic power consumption and thermal stress, particularly for higher operand sizes such as 256-bit, which are relevant for modern ECC standards [7,24].

Additionally, conventional Karatsuba implementations involve overlapping partial products during the reconstruction phase. The presence of these overlapping regions necessitates multi-level XOR trees, which increase logic depth and introduce glitching effects, further contributing to dynamic power dissipation [8,25]. As the operand size increases, this overlap-induced complexity becomes more pronounced, limiting scalability and energy efficiency [24,26].

2.2 Need for Architectural Exploration

While prior research has primarily focused on optimizing computational complexity, there is comparatively limited emphasis on understanding how architectural mapping influences power consumption. In FPGA-based systems, power is not solely determined by the number of logic elements, but also by the switching activity and temporal distribution of operations. Highly parallel architectures, despite offering low latency, activate a large number of logic blocks simultaneously, leading to peak power consumption [7,27].

- Power consumption increases rapidly with operand size in the instantiated architecture, while iterative designs exhibit more controlled, near-linear scaling.
- FSM-based resource sharing significantly reduces switching activity, the dominant contributor to dynamic power in FPGA implementations.
- The power-law model $P(n) = \alpha \cdot n^\beta + P_{static}$, fitted to synthesis data, yields $\beta \approx 1.58$ (instantiated) and $\beta \approx 1.54$ (iterative), both closely matching the Karatsuba theoretical exponent ($\log_2 3 \approx 1.585$). The $15\times$ lower α of the iterative design confirms that FSM-based resource sharing directly reduces switching activity without affecting algorithmic scaling.
- Architectural optimization has a greater impact on power efficiency than algorithmic complexity alone, especially for large-bit-width operations.
- No prior work reports power consumption for 256-bit GF(2^m) Karatsuba multipliers, establishing this as the first systematic characterization in the literature.

6. CONCLUSION

This work has demonstrated that architectural mapping decisions have a dominant and quantifiable impact on dynamic power consumption in FPGA-based 256-bit Karatsuba multipliers over GF(2^m). The iterative, FSM-controlled resource-shared architecture achieves an 89.5% reduction in estimated dynamic power (from 590.37 W to 62.00 W) relative to the fully instantiated parallel design, at the cost of a 90.1% increase in LUT utilization and an estimated latency of approximately 24 clock cycles per multiplication. *Note: These power values are Vivado post-synthesis estimates under worst-case switching activity (SA = 1.0) and are intended for relative architectural comparison only.*

The power-law curve fitting confirms that the scaling exponents $\beta \approx 1.58$ (instantiated) and $\beta \approx 1.54$ (iterative) both closely match the theoretical Karatsuba complexity ($\log_2 3 \approx 1.585$) for both architectures, while the FSM-based design achieves a $15\times$ reduction in the switching activity coefficient α . To the best of the authors' knowledge, this is the first reported systematic characterization of dynamic power for a 256-bit overlap-free Karatsuba multiplier on the Virtex-7 FPGA, addressing a gap that existing state-of-the-art works [24,33,34] do not fill. The GF(2^m) field choice provides inherent advantages for low-power FPGA realization through carry-free XOR-based arithmetic, and the iterative architecture makes this practical at 256-bit operand sizes relevant to both classical ECC and emerging post-quantum cryptographic applications [5,6,20,21].

FUTURE WORK

Future work will address the following directions:

- Extension to higher operand sizes (512-bit and 1024-bit) relevant to advanced ECC and PQC applications.
- Investigation of pipelining, clock-gating, and hybrid architectural techniques to enhance throughput while further reducing dynamic power.
- Post-implementation timing-aware FPGA analysis using VCD-based activity files for accurate absolute power and energy measurements.
- Integration into complete ECC scalar multiplication engines and PQC primitives.
- Broader benchmarking against GF(p) and PQC-based multipliers across different FPGA families and VLSI platforms.

AUTHOR CONTRIBUTIONS

CRedit: **R. RajaRaja**: Investigation; **V. R. Venkatasubramani**: Supervision; **A. Babu Karuppiyah**: Writing – review & editing; **S. Rajaram**: Validation

DISCLOSURE STATEMENT

No potential conflict of interest was reported by the author(s).

DECLARATION OF GENERATIVE AI AND AI-ASSISTED TECHNOLOGIES

During the preparation of this work, the authors used large language model (LLM) tools 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 it accurately reflects their own analysis and original contributions. The authors take full responsibility for the content of this publication.

DATA AVAILABILITY STATEMENT

All data generated or analyzed during this study are included in this article. Additional data are available from the corresponding author upon reasonable request.

REFERENCES

1. S. Raza, L. Seitz, D. Sitenkov, and G. Selander, "S3K: Scalable security with symmetric keys," *IEEE Trans. Autom. Sci. Eng.*, Vol. 13, no. 3, pp. 1270–80, 2016.
2. A. Mohammed, and N. Varol, "A Review Paper on Cryptography," in 2019 7th International Symposium on Digital Forensics and Security (ISDFS), June 2019, pp. 1–6, doi:10.1109/ISDFS.2019.8757514.

3. X. Zhou, and X. Tang, "Research and implementation of RSA algorithm for encryption and decryption," *Proc. IFOST*, Vol. 2, pp. 1118–21, 2011.
4. C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, "Elliptic curve lightweight cryptography: A survey," *IEEE Access.*, Vol. 6, pp. 72514–50, 2018.
5. K. Javeed, K. Saeed, and D. Gregg, "High-speed parallel reconfigurable Fp multipliers for elliptic curve cryptography applications," *Int. J. Circuit Theory Appl.*, Vol. 50, no. 4, pp. 1160–73, Apr. 2022.
6. K. Javeed, D. Irwin, and X. Wang, "Design and performance comparison of modular multipliers implemented on FPGA platform," in *Cloud Computing and Security. ICCCS 2016. Lecture Notes in Computer Science*, X. Sun, A. Liu, H.C. Chao, and E. Bertino, Ed. Springer, 2016. doi:10.1007/978-3-319-48671-0_23.
7. P. K. Meher, "Efficient FPGA implementation of low-complexity systolic Karatsuba multiplier over $GF(2^m)$ based on NIST polynomials," *IEEE Trans. CAS-I*, Vol. 64, no. 5, pp. 1243–56, May 2017.
8. H. Fan, J. Sun, M. Gu, and K. Y. Lam, "Overlap-free Karatsuba–Ofman polynomial multiplication algorithms," *IET Inf. Secur.*, Vol. 4, no. 1, pp. 8–14, Mar. 2010.
9. X. Zhang, J. Long, Z. Wang, and H. Cheng, "Lossless and reversible data hiding in encrypted images with public-key cryptography," *IEEE Trans. CSVT*, Vol. 26, no. 9, pp. 1622–31, 2016.
10. S. Banerjee, and A. Patil, "ECC based encryption algorithm for lightweight cryptography," in *Intelligent Systems Design and Applications. ISDA 2018 2018. Advances in Intelligent Systems and Computing*, vol. 940, A. Abraham, A.K. Cherukuri, P. Melin, and N. Gandhi, Ed. Springer, 2020, pp. 600–9. doi:10.1007/978-3-030-16657-1_56.
11. T. Shimada, and M. Ikeda, "High-throughput polynomial multiplier architecture for lattice-based cryptography," in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, Daegu, Korea, 2021, pp. 1–5. doi:10.1109/ISCAS51556.2021.9401755.
12. Y. Cui, Y. Zhang, Z. Ni, S. Yu, C. Wang and W. Liu, "High-throughput polynomial multiplier for accelerating Saber on FPGA," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, Vol. 70, no. 9, pp. 3584–3588, 2023. doi:10.1109/TCSII.2023.3264803.
13. X. Hu, J. Tian, M. Li, and Z. Wang, "AC-PM: An area-efficient and configurable polynomial multiplier for lattice-based cryptography," *IEEE Trans. CAS-I*, vol. 70, no. 2, pp. 719–732, Feb. 2023. doi:10.1109/TCSI.2022.3218192.
14. J. Wang, C. Yang, F. Zhang, Y. Meng, S. Xiang, and Y. Su, "High-throughput Toom–Cook-4 polynomial multiplier for lattice-based cryptography," *IEEE Trans. CAS-I*, Vol. 71, no. 1, pp. 359–72, 2024.
15. Y. A. Birgani, S. Timarchi, and A. Khalid, "Area-time-efficient scalable schoolbook polynomial multiplier for lattice-based cryptography," *IEEE Trans. CAS-II*, Vol. 69, no. 12, pp. 4957–61, 2022.
16. K.J. Jegadish Kumar, P. Kaythry, V. Gokhulesh, and K. Sudharsan, "Efficient FPGA implementation of RSA using Vedic multiplier," in *2023 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET), Chennai, India*, 1–5, 2023. doi:10.1109/WiSPNET57748.2023.10134210.
17. P. Kodali, S. S. Yenamachintala, and L. Boppana, "FPGA implementation of 160-bit Vedic multiplier," in *2014 International Conference on Devices, Circuits and Communications (ICDCCom), Ranchi, India*, 1–5, 2014. doi:10.1109/ICDCCom.2014.7024721.
18. R. Ahuja, H. Soni, and K. Bhavsar, "Fast, secure and efficient Vedic approach for cryptographic FPGA implementations on FPGA," *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India*, 1706–10, 2018. doi:10.1109/ICECA.2018.8474569.
19. G. Leelavathi, K. Shaila, and K.R. Venugopal, "Elliptic curve crypto processor on FPGA using Montgomery multiplication with Vedic and encoded multiplier over $GF(2^m)$ for nodes in wireless sensor networks," in *2018 IEEE 13th International Conference on Industrial and Information Systems (ICIIS), Rupnagar, India*, 207–10, 2018. doi:10.1109/ICIINFS.2018.8721398.
20. K. Javeed, S. Rubab, and D. Gregg, "Efficient reconfigurable modular multipliers for post-quantum digital signatures," in *2024 31st IEEE International Conference on Electronics, Circuits and Systems (ICECS), Nancy, France*, 2024, 1–4. doi: 10.1109/ICECS61496.2024.10849189.
21. Y. A. Shah, C. Rafferty, A. Khalid, S. Khan, K. Javeed, and M. O'Neill, "Efficient soft core multiplier for post-quantum digital signatures," *Proc. IEEE ISCAS*, May 2024.
22. A. Percey, "Advantages of the Virtex-5 FPGA 6-input LUT architecture," Xilinx White Paper WP284, 2007.
23. D. Pamula, and A. Tisserand, "Fast and secure finite field multipliers," in *2015 Euromicro Conference on Digital System Design, Madeira, Portugal*, 2015, 1–8. doi: 10.1109/DSD.2015.46.
24. M. Heidarpur, and M. Mirhassani, "An efficient and high-speed overlap-free Karatsuba-based finite-field multiplier

- for FPGA implementation,” *IEEE Trans. VLSI Syst.*, Vol. 29, no. 4, pp. 667–76, Apr. 2021.
25. A. D. Piccoli, A. Visconti, and O. G. Rizzo, “Polynomial multiplication over binary finite fields: New upper bounds,” *J. Cryptographic Eng.*, Vol. 10, pp. 197–210, 2019.
 26. Y. Li, Y. Zhang, and W. He, “Fast hybrid Karatsuba multiplier for type-II pentanomials,” *IEEE Trans. VLSI Syst.*, Vol. 28, no. 11, pp. 2459–63, 2020.
 27. Z. U. A. Khan, and M. Benaissa, “High-speed and low-latency ECC processor over GF(2^m) on FPGA,” *IEEE Trans. VLSI Syst.*, Vol. 25, no. 1, pp. 165–76, 2017.
 28. R. K. Agrawal, and H. M. Kittur, “ASIC-based logarithmic multiplier using iterative pipelined architecture,” in *2013 IEEE Conference on Information & Communication Technologies, Thuckalay, India, 2013*, pp. 362–6. doi: 10.1109/CICT.2013.6558121.
 29. T. Krishnan, and S. Saravanan, “Design of low-area and high-speed pipelined single-precision floating-point multiplier,” in *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2020*, pp. 1259–64. doi: 10.1109/ICACCS 48705.2020.9074366.
 30. H. Zhang, D. Chen, and S.-B. Ko, “Area- and power-efficient iterative single/double-precision merged floating-point multiplier on FPGA,” *IET CDT*, Vol. 11, no. 4, pp. 149–58, 2017.
 31. P. Hosseinzadeh Namin, C. Roma, R. Muscedere, and M. Ahmadi, “Efficient VLSI implementation of a sequential finite-field multiplier using reordered normal basis,” *IEEE Trans. VLSI Syst.*, Vol. 26, no. 11, pp. 2542–52, 2018.
 32. S. Karthikeyan, and M. Jagadeeswari, “Performance improvement of ECC using low-power, high-speed 16×16 Vedic multiplier based on reversible logic,” *J. Ambient Intell. Humaniz. Comput.*, Vol. 12, pp. 4161–70, 2021.
 33. R. Kumari, G. Purohit, and A. Karmakar, “Efficient hardware implementation of modular multiplier over GF(2^m) on FPGA,” in *Proc. 2nd Int. Conf. Intelligent Systems and Signal Processing (ISSP), Lecture Notes in Electrical Engineering*, vol. 1210, Springer, pp. 257–271, 2023.
 34. M. Thirumoorthi, A. J. Leigh, M. Heidarpur, M. Khalid, and M. Mirhassani, “Novel formulations of M-term overlap-free Karatsuba binary polynomial multipliers and their hardware implementations,” *IEEE Trans. VLSI Syst.*, Vol. 31, no. 10, pp. 1509–22, Oct. 2023.

AUTHORS



R RajaRaja received the BE degree in electronics and communication engineering from Bannari Amman Institute of Technology, Sathyamangalam, India, in 2011, and the ME degree in VLSI design from SSN College of Engineering, Chennai, India, in 2013. He is currently working as an assistant professor at the PSG Institute of Technology and Applied Research, Coimbatore, India. He is presently pursuing the PhD degree at Thiagarajar College of Engineering, Madurai, under Anna University, Chennai. His research interests include VLSI design and cryptography.

Corresponding author. birneraja@gmail.com



V R Venkatasubramani received the AMIE degree in electronics and communication engineering from The Institution of Engineers (India) in 1999, the ME degree in optical communication from AC. College of Engineering and Technology, Karaikudi, India, in 2005, and the PhD degree in cryptographic hardware from Thiagarajar College of Engineering, Madurai, under Anna University, Chennai, in 2015. He is currently working as an associate professor in the Department of Electronics and Communication Engineering, Thiagarajar College of Engineering, Madurai, India. His research interests include cryptographic hardware architectures, elliptic curve cryptography, finite-field arithmetic, FPGA-based security processors, and low-power VLSI design. He has published extensively in reputed international journals and conferences and has guided several post-graduate and doctoral research scholars in the area of hardware security and VLSI systems.

Email: venthiru@tce.edu



A Babu Karuppiah received BE, and ME degrees in electronics and communication engineering. He received his PhD degree from Anna University, Chennai. He is currently working as a professor in the Department of Electronics and Communication Engineering at Sri Eshwar College of Engineering, Coimbatore. His research interests include wireless sensor networks, internet of things, VLSI architectures and secure embedded system design. He has actively guided student projects addressing socially relevant engineering problems and has served as a principal investigator for several funded research projects supported by government agencies. His work has received recognition at district and national levels, and he has contributed to applied research in e-health systems, IoT-based safety solutions, and smart monitoring applications. He holds patents in his areas of research and has been involved in organizing and participating in technical training programmes and faculty development initiatives.

Email: babkarofficial@gmail.com



S Rajaram received the BE degree in electronics and communication engineering from Thiagarajar College of Engineering, Madurai, the ME degree in microwave and optical engineering, and the PhD degree in VLSI Design. He also carried out post-doctoral research in 3D wireless system design at Georgia Institute of Technology, Atlanta, USA. He is currently working as a professor in the Department of Electronics and Communication Engineering, Thiagarajar College of Engineering, Madurai. His research interests include VLSI physical design, low-power integrated circuits, FPGA-based architectures, cryptographic hardware, wireless communication systems, and secure embedded systems. He has guided several doctoral and postgraduate research scholars and has contributed extensively to research in integrated circuit design and hardware security.

Email: rajaram_siva@tce.edu