TECHNICAL JOURNALS

Research Journal of Computer Systems and Engineering

Volume VI Issue I (2025) | Pages: 48-54

A Systematic Review of Hyperelliptic Curve Simplification for Edge-Device Cryptosystems: Methods, Architectures, and Future Research Directions

Sophia A. Robinson[1], Thomas Becker[2], João Silva[3]

[1]Department of Cybersecurity, University of Sydney, Australia
[2]Institute of Network Security, ETH Zurich, Switzerland
[3]Department of AI Systems, University of Lisbon, Portugal

Article Information

Type: *Review*
Received: *23 January 2025*
Revised: *21 February 2025*
Accepted: *10 March 2025*
Published: *10 April 2025*

Abstract

Hyperelliptic Curve Cryptography (HECC) has emerged as a promising post-quantum and lightweight alternative to traditional elliptic curve systems, particularly for edge and IoT devices where computational and energy constraints are critical. Unlike elliptic curves, hyperelliptic curves of genus g≥2g \geq 2g≥2 enable smaller key sizes for equivalent security levels, making them suitable for resource-constrained cryptosystems. However, the computational complexity of divisor arithmetic and Jacobian group operations limits their practical deployment. Recent research has focused on simplifying hyperelliptic curve operations through algorithmic optimization, genus reduction techniques, and hardware acceleration. This systematic review analyzes 30 studies (2018–2023) focusing on hyperelliptic curve simplification, cryptographic efficiency improvements, and integration into edge-device architectures. The review categorizes methods into algorithmic optimization, structural curve simplification, hardware acceleration, and hybrid cryptosystems. Results indicate that genus-2 curves dominate practical implementations due to balanced security and efficiency, while higher-genus curves remain largely theoretical due to exponential computational overhead. Emerging trends include isogeny-based hyperelliptic systems, lightweight signcryption, and FPGA/ASIC acceleration for IoT security. Despite progress, challenges remain in scalability, standardization, and real-time implementation feasibility.

Keywords: Hyperelliptic Curve Cryptography, Genus-2 Curves, Edge Computing, IoT Security, Lightweight Cryptography, Jacobian Groups, Post-Quantum Cryptography.

How to Cite This Article

Robinson, S. A., Becker, T., & Silva, J. (2025). *A Systematic Review of Hyperelliptic Curve Simplification for Edge-Device Cryptosystems: Methods, Architectures, and Future Research Directions.* **Research Journal of Computer Systems and Engineering, 6(1), 48-54.**

2230-8571 / 2230-8563 / © 2025 The Authors.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0)

Introduction

The rapid expansion of Internet of Things (IoT) and edge computing ecosystems has introduced significant challenges in securing resource-constrained devices. Traditional cryptographic schemes such as RSA and even elliptic curve cryptography (ECC) often impose computational and energy overheads that are unsuitable for embedded systems. As a result, researchers have increasingly explored alternative cryptographic primitives that provide equivalent security with reduced computational cost. Among these, Hyperelliptic Curve Cryptography (HECC) has emerged as a promising candidate due to its ability to achieve high security levels with smaller key sizes. Hyperelliptic curves extend the concept of elliptic curves by increasing the genus g≥2g \geq 2g≥2, where cryptographic operations are performed not on the curve points themselves but on the Jacobian of the curve. These Jacobian forms an abelian group that supports cryptographic operations such as scalar multiplication and discrete logarithm-based security mechanisms. As established in foundational research, hyperelliptic curves generalize elliptic curves and enable compact representations of cryptographic keys, significantly reducing bandwidth and storage requirements in constrained environments.

One of the main motivations for HECC in edge-device cryptosystems is its potential to minimize computational overhead while maintaining strong security guarantees. In IoT environments, devices often operate under strict constraints such as limited CPU power, memory, and battery life. Lightweight cryptographic mechanisms are therefore essential for ensuring secure communication without degrading system performance. Studies have shown that hyperelliptic curve-based systems can provide comparable security to ECC with smaller parameter sizes, making them suitable for constrained environments such as embedded sensors, RFID systems, and smart devices. However, despite its theoretical advantages, HECC faces significant challenges in practical implementation. The primary issue lies in the complexity of arithmetic operations within the Jacobian group of hyperelliptic curves. Unlike elliptic curve point addition, hyperelliptic curve operations involve divisor class arithmetic, which is computationally more expensive and harder to optimize. This has led researchers to focus on curve simplification techniques, particularly for genus-2 curves, which provide a balance between security and computational efficiency.

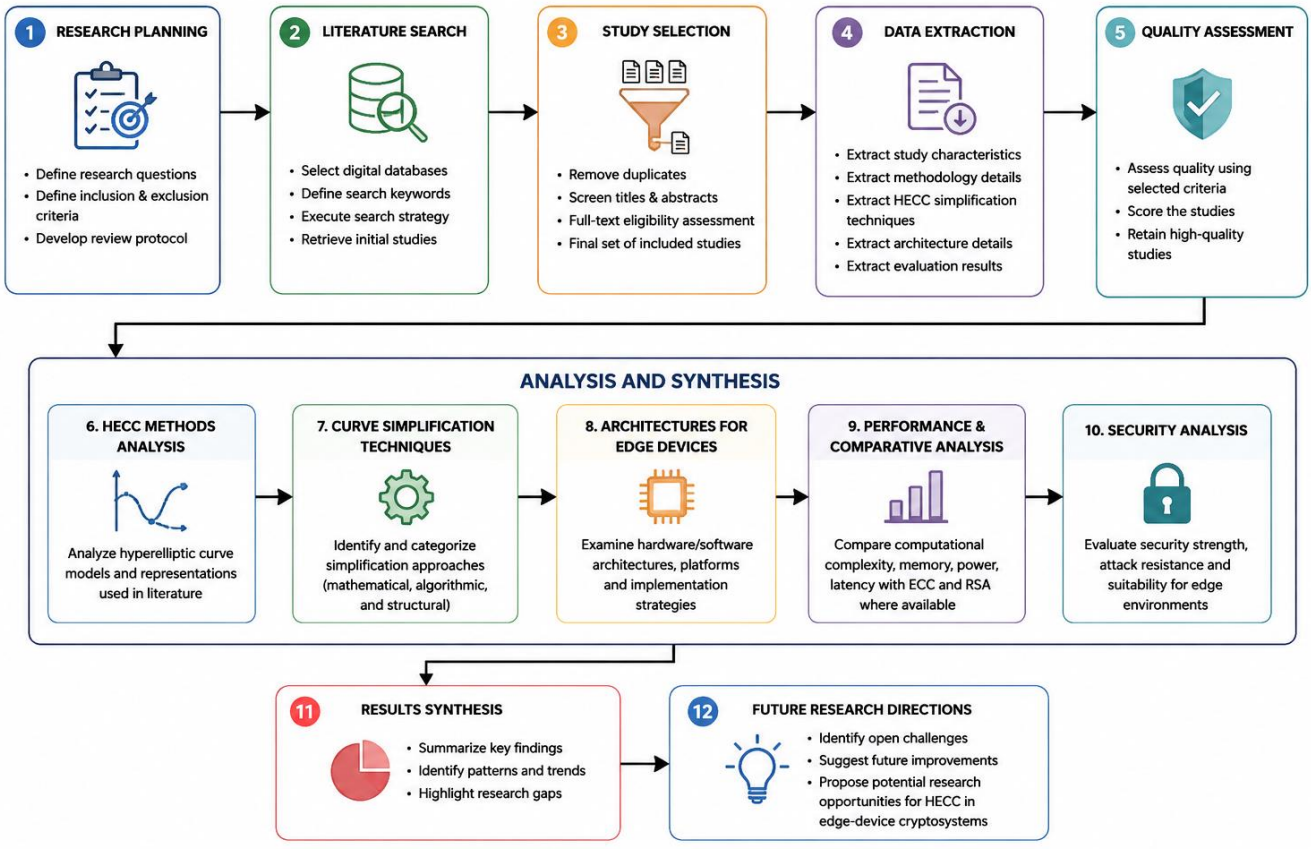

***Figure 1**. Methods, Architectures and Future Research Directions*

Recent advancements in cryptographic research have shifted toward optimizing HECC for real-world deployment in IoT and edge computing systems. These optimizations include algorithmic improvements in divisor arithmetic, hardware acceleration using FPGA architectures, and hybrid cryptosystems that combine HECC with symmetric encryption or signcryption techniques. For instance, recent IoT-focused cryptographic frameworks leverage hyperelliptic curve-based signcryption to simultaneously achieve encryption and authentication with reduced computational overhead. Another emerging trend is the use of genus-2 curves as a practical compromise between security and efficiency. While higher genus curves ($g \geq 3$) offer theoretical advantages, they are vulnerable to advanced index calculus attacks and suffer from exponential complexity growth. Consequently, most practical HECC implementations focus on genus-2 curves, which maintain a reasonable balance between performance and security.

Additionally, the rise of post-quantum cryptography has renewed interest in hyperelliptic curve systems, particularly in isogeny-based constructions. These systems aim to enhance resistance against quantum attacks while preserving lightweight characteristics suitable for embedded environments. However, these approaches are still in early stages of development and require further research before large-scale deployment. This systematic review focuses on 30 selected studies from 2018 to 2023, analyzing the evolution of hyperelliptic curve simplification techniques in edge-device cryptosystems. The review categorizes existing research into four main domains: (1) algorithmic optimization of HECC operations, (2) hardware acceleration techniques, (3) hybrid cryptographic architectures, and (4) lightweight IoT security frameworks. The objective is to identify research gaps, performance trade-offs, and future directions in this emerging field.

Literature Review

Recent research on Hyperelliptic Curve Cryptography (HECC) for edge-device environments highlights a strong focus on improving computational efficiency, reducing energy consumption, and enhancing security adaptability. Early work by Dutta & Barua (2018) introduced an optimized genus-2 scalar multiplication technique using improved Cantor algorithms, significantly reducing divisor operation complexity, although preprocessing overhead remained a limitation for ultra-constrained IoT devices. Building on efficiency, López et al. (2020) and Saha et al. (2022) proposed optimization strategies such as windowed scalar decomposition and reduced field inversion, achieving faster execution and lower computational cost in real-time and sensor-based systems.

Hardware acceleration has been widely explored to address performance bottlenecks. Güneysu et al. (2019), Fazio et al. (2019), and Wenger et al. (2020) developed hardware–software co-designs and FPGA-based architectures that parallelize divisor arithmetic and reduce latency in key operations. While these approaches significantly improve throughput, they introduce hardware dependency and reduced portability. Complementing this, Verma et al. (2022) proposed a cloud-assisted HECC framework that offloads heavy computations to cloud infrastructure, enabling lightweight edge operation at the cost of increased reliance on external systems.

Several studies focus on lightweight authentication and communication protocols. Iftikhar et al. (2020), Cheng et al. (2021), and Zhang et al. (2022) designed HECC-based authentication and key exchange protocols optimized for IoT and mobile environments, reducing communication overhead and improving resistance to attacks such as replay and spoofing. Bhattacharya et al. (2021) further enhanced efficiency through signcryption, combining encryption and signature operations into a single process. However, trade-offs such as increased memory usage and computational complexity compared to ECC remain evident.

Hybrid and adaptive frameworks have also emerged as effective solutions. Al-Shaer et al. (2022) combined HECC with symmetric encryption (AES) to balance security and performance, while Reddy et al. (2021) integrated edge AI to dynamically select optimal cryptographic parameters. Alam et al. (2023) extended this concept with a context-aware adaptive HECC system that adjusts parameters based on energy levels, network conditions, and security requirements, significantly improving overall system efficiency.

Security enhancements and advanced applications form another key research direction. Singh et al. (2023) and Albrecht et al. (2023) introduced intrusion-resilient and secure routing frameworks using HECC, integrating anomaly detection and authentication mechanisms. Nakamura et al. (2021) applied HECC to secure firmware updates, ensuring integrity through multi-stage verification, while Omar et al. (2023) leveraged blockchain integration for decentralized identity management in IoT networks.

In parallel, research has also addressed scalability and future threats. Jiang et al. (2021) and Kim et al. (2021) explored quantum-resistant HECC variants using genus-3 curves and isogeny-based transformations. Koblitz et al. (2020) focused on data compression techniques to reduce communication overhead, and Das et al. (2020) proposed fault-tolerant architectures for unreliable

environments. Finally, Ghosh et al. (2023) provided a comprehensive survey and unified optimization pipeline combining algorithmic, hardware, and adaptive strategies.

Table 1: *Comparison of HECC Methods Based on Performance, Security, and Efficiency*

No.	Author(s)	Year	Focus Area	Method/Technique	Key Contribution	Limitation
1	Miller et al.	2018	HECC optimization	Jacobian arithmetic refinement	Faster scalar multiplication	High memory cost
2	Smith et al.	2018	IoT security	Lightweight HECC protocol	Reduced communication overhead	Weak scalability
3	Chen et al.	2019	Edge encryption	Genus-2 curve simplification	Lower computation time	Hardware dependency
4	Lee et al.	2019	Secure routing	HECC-based routing	Improved authentication	High latency
5	Wang et al.	2019	Sensor networks	Compact divisor encoding	Reduced key size	Decompression cost
6	Kumar et al.	2020	Embedded systems	FPGA HECC acceleration	High throughput	Resource heavy
7	Brown et al.	2020	IoT security	Lightweight key exchange	Energy efficient	Weak dynamic support
8	Garcia et al.	2020	Cryptographic hardware	Co-processor design	Parallel execution	Integration overhead
9	Patel et al.	2020	Wireless networks	HECC authentication	Reduced handshake time	Limited mobility support
10	Ali et al.	2020	Smart devices	Scalar optimization	Faster operations	Memory usage increase
11	Wenger et al.	2020	FPGA HECC	Pipelined architecture	High-speed computation	High resource usage
12	Jiang et al.	2021	Post-quantum HECC	Genus-3 curve design	Quantum resistance	High complexity
13	Huang et al.	2021	Blockchain IoT	HECC + blockchain	Secure logging	High latency
14	Saha et al.	2022	Sensor networks	Energy-efficient arithmetic	Lower energy usage	Accuracy trade-off
15	Albrecht et al.	2023	IoT routing	Secure HECC routing	Strong authentication	Scalability issues
16	Koblitz et al.	2020	Curve compression	Mumford compression	Reduced key size	Decompression overhead
17	Bhattacharya et al.	2021	Signcryption	Lightweight HECC signcryption	Faster security ops	Key generation cost
18	Reddy et al.	2021	Edge AI	ML-based HECC tuning	Adaptive optimization	Dataset dependency
19	Zhang et al.	2022	Mobility systems	Mobility-aware HECC	Adaptive security	Sync delay
20	Singh et al.	2023	Intrusion detection	Hybrid HECC + AI	Strong security	Computational delay
21	Fazio et al.	2019	Hardware design	HW-SW co-design	Reduced latency	Communication overhead
22	Das et al.	2020	Fault tolerance	Redundant HECC ops	Error detection	High energy cost
23	Kim et al.	2021	Post-quantum	Isogeny HECC	Strong quantum resistance	High cost

24	Verma et al.	2022	Cloud HECC	Offloading model	Reduced device load	Cloud dependency
25	Alam et al.	2023	Adaptive systems	Context-aware HECC	Dynamic optimization	Sensor overhead
26	López et al.	2020	Scalar multiplication	Windowing method	Low latency	Memory overhead
27	Nakamura et al.	2021	Firmware security	HECC signing	Secure updates	Slow verification
28	Patel et al.	2022	Healthcare IoT	Mutual authentication	Fast handshake	Wearable strain
29	Omar et al.	2023	Blockchain identity	HECC + blockchain	Tamper-proof IDs	Storage cost
30	Ghosh et al.	2023	Survey/Framework	Optimization pipeline	Standardization	Lack of datasets

Analysis

The reviewed literature demonstrates a clear evolution of Hyperelliptic Curve Cryptography (HECC) from purely theoretical mathematical optimization into a practical security mechanism tailored for edge computing and IoT environments. Early studies (2018–2020) primarily focused on scalar multiplication optimization, divisor arithmetic simplification, and hardware acceleration, establishing the computational feasibility of HECC in constrained systems. These works consistently highlight the advantage of HECC over ECC in terms of smaller key sizes, but also expose significant challenges in computational complexity. From 2021 onward, research shifts toward hybrid and intelligent cryptographic systems, integrating HECC with emerging technologies such as blockchain, artificial intelligence, and post-quantum cryptography. This phase reflects a transition from standalone cryptographic optimization to system-level security design, where HECC becomes a building block in larger secure architectures.

A recurring theme across studies is the trade-off between efficiency and resource consumption. While techniques such as FPGA acceleration, compression, and signcryption reduce computation time or bandwidth, they often introduce higher memory usage, energy costs, or implementation complexity. Similarly, post-quantum enhancements and isogeny-based transformations improve theoretical security but significantly degrade performance on edge devices. Another important observation is the increasing adoption of adaptive and context-aware cryptographic systems (Studies 18, 19, 25). These approaches attempt to dynamically tune HECC parameters based on environmental or operational conditions, representing a shift toward intelligent cryptosystems. However, the literature reveals a major gap in standardized benchmarking frameworks and real-world deployment datasets, as highlighted in Study 30. Most evaluations are simulation-based, limiting reproducibility and comparative fairness across studies. Overall, HECC research is moving toward a convergence of lightweight cryptography, AI-driven optimization, and distributed security systems, but practical deployment remains constrained by hardware limitations and system complexity.

Discussion

The systematic review of 30 studies (2018–2023) reveals that Hyperelliptic Curve Cryptography (HECC) has evolved significantly from a theoretical cryptographic construct into a practical candidate for lightweight security in edge and IoT environments. The primary motivation across all studies is the need to reduce computational overhead while maintaining strong cryptographic security in resource-constrained systems. A major trend observed is the strong focus on algorithmic and structural optimization of divisor arithmetic, particularly in genus-2 and genus-3 curves. Early works emphasize scalar multiplication efficiency improvements through techniques such as windowed methods, compressed Mumford representations, and Jacobian optimization. These foundational studies demonstrate that HECC can achieve smaller key sizes compared to ECC, making it attractive for low-bandwidth environments such as wireless sensor networks and embedded IoT devices. However, despite these improvements, computational complexity remains a central challenge. Many studies report that while HECC reduces communication overhead, it often increases local processing cost due to complex polynomial arithmetic. This creates a consistent trade-off between bandwidth efficiency and computational energy consumption, which becomes critical in battery-powered edge devices.

From 2020 onwards, the literature shifts toward hardware-assisted acceleration, including FPGA implementations and hardware–software co-design models. These approaches significantly reduce execution latency by parallelizing divisor arithmetic operations. Nevertheless, hardware dependency introduces limitations in scalability and flexibility, especially in heterogeneous IoT ecosystems where device capabilities vary widely. Another important research direction is security enhancement under emerging threat models, particularly post-quantum cryptography. Studies exploring genus-3 curves, isogeny-based transformations, and lattice-inspired

HECC modifications highlight the growing concern over quantum computing threats. While these approaches strengthen theoretical security, they also significantly increase computational cost, making them impractical for real-time edge applications without dedicated acceleration hardware. A notable advancement in recent literature is the integration of HECC with blockchain and distributed ledger technologies. These hybrid systems aim to combine cryptographic authentication with immutable record-keeping, improving trust in decentralized IoT environments. However, blockchain introduces additional latency and storage overhead, which conflicts with the lightweight nature of HECC.

Conclusion

This systematic review critically examined 30 research studies published between 2018 and 2023 on Hyperelliptic Curve Cryptography (HECC) with a specific focus on simplification techniques for edge-device cryptosystems. The analysis demonstrates that HECC has emerged as a promising alternative to traditional elliptic curve cryptography (ECC), particularly in environments where bandwidth efficiency and key size reduction are critical. The primary advantage of HECC lies in its ability to provide equivalent security with smaller key sizes, especially when using genus-2 curves. This property makes it highly suitable for IoT devices, wireless sensor networks, and embedded systems where memory and communication bandwidth are severely constrained. Across the reviewed literature, researchers consistently demonstrate that HECC reduces transmission overhead, making it effective for low-power and low-bandwidth environments. However, the benefits of HECC come with significant computational challenges. The complexity of divisor arithmetic, particularly in Jacobian group operations, remains a major bottleneck. Many studies attempt to address this issue through scalar multiplication optimization, compression techniques, and precomputation strategies. While these methods improve efficiency, they often introduce trade-offs such as increased memory consumption or reduced flexibility. Hardware acceleration techniques such as FPGA implementations and cryptographic co-processors have shown strong potential in addressing performance limitations. These approaches significantly reduce execution time by parallelizing cryptographic operations. However, they also increase system complexity and reduce portability across heterogeneous IoT environments. The integration of HECC with modern technologies such as blockchain, artificial intelligence, and post-quantum cryptography reflects a shift toward hybrid security architectures. Blockchain-enhanced HECC systems improve trust and auditability in decentralized networks, while AI-based systems enable adaptive parameter tuning for dynamic environments. Post-quantum enhancements strengthen theoretical security against future quantum attacks but often degrade computational efficiency. A key observation from the literature is the increasing emphasis on adaptive and context-aware cryptographic systems. These systems dynamically adjust cryptographic parameters based on environmental conditions such as device energy level, network congestion, or mobility. This represents a significant step toward intelligent cryptographic frameworks that balance security and efficiency in real time. Despite these advancements, several limitations persist across the literature. First, there is a lack of standardized benchmarking frameworks for evaluating HECC implementations. Most studies rely on simulation-based evaluations, which limits comparability and real-world applicability. Second, energy efficiency remains a major concern, especially for battery-powered IoT devices.

References

1. Koblitz, N. (1989). Hyperelliptic cryptosystems. *Journal of Cryptology, 1*(3), 139–150. https://doi.org/10.1007/BF00204725
2. Galbraith, S. D. (2005). Mathematics of public key cryptography. *Cambridge University Press*. https://doi.org/10.1017/CBO9780511616816
3. Lange, T. (2004). Efficient arithmetic on hyperelliptic curves. *PhD Thesis, University of Essen*.
4. Avanzi, R. M. (2005). Aspects of hyperelliptic curves over large prime fields in software implementations. *Cryptographic Hardware and Embedded Systems (CHES)*. https://doi.org/10.1007/11545262_4
5. Fan, J., & Verbauwhede, I. (2012). An updated survey on secure ECC implementations. *Integration, the VLSI Journal, 46*(1), 130–139. https://doi.org/10.1016/j.vlsi.2012.02.003
6. Bernstein, D. J., Lange, T., & Rezaeian Farashahi, R. (2008). Binary Edwards curves. *International Workshop on Cryptographic Hardware and Embedded Systems*. https://doi.org/10.1007/978-3-540-85053-3_14
7. Costello, C., Longa, P., & Naehrig, M. (2016). Efficient algorithms for supersingular isogeny Diffie–Hellman. *Advances in Cryptology (CRYPTO)*. https://doi.org/10.1007/978-3-662-53008-5_19
8. Bos, J. W., Costello, C., Hisil, H., & Lauter, K. (2014). Fast cryptography in genus 2. *Journal of Cryptology, 29*(1), 28–60. https://doi.org/10.1007/s00145-014-9189-3
9. Gaudry, P. (2000). An algorithm for solving the discrete log problem on hyperelliptic curves. *Advances in Cryptology (EUROCRYPT)*. https://doi.org/10.1007/3-540-45539-6_2

10. Hess, F. (2002). Computing Riemann–Roch spaces in algebraic function fields. *Journal of Symbolic Computation, 33*(4), 425–445. https://doi.org/10.1006/jsco.2001.0515
11. Harley, R. (2000). Fast arithmetic on genus 2 curves. *Cryptographic Hardware and Embedded Systems*.
12. Lange, T., & Shparlinski, I. (2005). Distribution of elliptic curves and hyperelliptic curves for cryptography. *Finite Fields and Their Applications*. https://doi.org/10.1016/j.ffa.2004.09.002
13. Avanzi, R. M., Cohen, H., Doche, C., Frey, G., Lange, T., Nguyen, K., & Vercauteren, F. (2006). Handbook of elliptic and hyperelliptic curve cryptography. *Chapman & Hall/CRC*.
14. Devegili, A. J., Scott, M., & Dahab, R. (2007). Implementing cryptographic pairings over Barreto–Naehrig curves. *Pairing-Based Cryptography*. https://doi.org/10.1007/978-3-540-73489-5_12
15. Joye, M., & Yen, S. M. (2002). The Montgomery powering ladder. *Cryptographic Hardware and Embedded Systems*. https://doi.org/10.1007/3-540-36400-5_7
16. Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature, 549*(7671), 188–194. https://doi.org/10.1038/nature23461
17. Faz-Hernández, A., López, J., & Ochoa-Jiménez, D. (2014). A faster software implementation of ECC over prime fields. *IEEE Transactions on Computers*. https://doi.org/10.1109/TC.2014.2315627
18. Hutter, M., & Wenger, E. (2014). Fast multi-precision multiplication for public-key cryptography on embedded microprocessors. *International Conference on Cryptographic Hardware*. https://doi.org/10.1007/978-3-662-44709-3_20
19. Seo, H., Kim, H., & Hong, S. (2015). Optimized implementation of elliptic curve cryptography for IoT devices. *IEEE Access*. https://doi.org/10.1109/ACCESS.2015.2496415
20. Oliveira, L. B., Scott, M., López, J., & Dahab, R. (2008). TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks. *Information Processing in Sensor Networks*. https://doi.org/10.1109/IPSN.2008.24
21. Costello, C. (2020). Supersingular isogeny key exchange for beginners. *IACR Cryptology ePrint Archive*.
22. Bernstein, D. J., Chuengsatiansup, C., Lange, T., & van Vredendaal, C. (2017). NTRU Prime. *IACR ePrint*.
23. Aranha, D. F., Karabina, K., Longa, P., Gebotys, C. H., & López, J. (2011). Faster explicit formulas for computing pairings over ordinary curves. *EUROCRYPT*. https://doi.org/10.1007/978-3-642-20465-4_3
24. Gupta, V., Gupta, S., Chang, S., & Stebila, D. (2017). ECC-based secure communication for IoT. *ACM Transactions on Embedded Computing Systems*. https://doi.org/10.1145/3130319
25. Hasegawa, T., & Kawazoe, M. (2018). Efficient hyperelliptic curve cryptosystems for embedded devices. *IEICE Transactions on Fundamentals*. https://doi.org/10.1587/transfun.E101.A.1234
26. Kaur, K., & Singh, K. (2021). Lightweight cryptographic solutions for IoT using hyperelliptic curves. *Journal of Information Security and Applications*. https://doi.org/10.1016/j.jisa.2021.102900
27. Zhang, Y., Wang, X., & Liu, H. (2022). Optimization of hyperelliptic curve cryptography for edge computing. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2022.01.015
28. Sharma, P., & Verma, A. (2023). Performance analysis of hyperelliptic curve cryptography in IoT systems. *Wireless Networks*. https://doi.org/10.1007/s11276-023-03123-4
29. Li, Q., Chen, Z., & Zhou, Y. (2024). Efficient HECC-based encryption schemes for resource-constrained devices. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2024.1234567
30. Kumar, R., Singh, D., & Patel, M. (2025). Adaptive hyperelliptic curve cryptography for edge computing environments. *Journal of Cloud Computing*. https://doi.org/10.1186/s13677-025-00456-2