Karshi Multidisciplinary International Scientific Journal

www.kmisj.reapress.com

K. Multidiscip. Int. Sci. J. Vol. 2, No. 3 (2025) 160–168.

Paper Type: Original Article

Performance Evaluation of Lightweight Cryptography Hybrid Algorithms for Data Security

Siddeshwari Patil[1,*], Rajesh Bansode[1]

[1] Department of Information Technology, Thakur College of Engineering & Technology, Mumbai, Maharashtra, IN; patilsiddi123@gmail.com; rajesh.bansode@tcetmumbai.in.

Citation:

Received: 12 March 2025 *Revised: 19 May 2025* *Accepted: 27 July 2025*	Patil, S., & Bansode, R. (2025). Performance evaluation of lightweight cryptography hybrid algorithms for data security. *Karshi multidisciplinary international scientific journal, 2*(3), 160-168.

Abstract

With the rapid expansion of digital communication and data exchange, ensuring data security has become paramount. Traditional cryptographic methods often struggle with balancing security, efficiency, and lightweight implementation for resource-constrained environments. This research focuses on the performance analysis and development of a lightweight cryptographic algorithm for enhanced data security by implementing Simon, Speck, and ChaCha20 individually, as well as in hybrid combinations—Simon-ChaCha20 and Speck-ChaCha20. A key research gap addressed is the need for cryptographic solutions that offer high security while maintaining computational efficiency for diverse data types. The main objective is to evaluate these algorithms based on their avalanche effect, encryption, and decryption performance across different data types, including text, audio, video, and document files. The entire methodology involves implementing and testing the individual and hybrid algorithms, analyzing their avalanche scores for text data, and comparing encryption and decryption times for various file formats. Results of this work indicate that hybrid algorithms achieve a higher avalanche score, demonstrating enhanced security, while also being adaptable for multimedia data encryption. The study's findings have significant implications for lightweight cryptographic applications in Internet of Things (IoT), embedded systems, and real-time secure communication, offering a robust and efficient encryption approach for modern cybersecurity challenges.

Keywords: Lightweight encryption, Simon cipher, Hybrid cryptography, Avalanche effect, Resource-efficient security.

1 | Introduction

As digital systems continue to evolve, protecting sensitive information is more critical than ever, especially in environments with limited resources, such as Internet of Things (IoT) devices and low-power embedded systems. Traditional encryption methods, like Advanced Encryption Standard (AES) and RSA, though highly

Corresponding Author: patilsiddi123@gmail.com

https://doi.org/10.22105/kmisj.v2i3.70

secure, require significant processing power and memory, making them less practical for devices with constrained resources [1]. To address these limitations, lightweight cryptographic algorithms have been developed, balancing security and efficiency to meet the demands of such environments.

This study examines three lightweight cryptographic algorithms: Simon, Speck, and ChaCha20. Simon and Speck, designed by the National Security Agency (NSA), are block ciphers optimized for simplicity and low resource consumption. ChaCha20, a stream cipher created by Daniel J. Bernstein, offers strong security and high performance even in resource-constrained systems. In addition to evaluating these individual algorithms, the research explores hybrid cryptographic methods by combining Simon with ChaCha20 and Speck with ChaCha20, forming hybrid models named Simon-ChaCha20 and Speck-ChaCha20 [2].

The avalanche effect was used as a key performance metric, measuring how effectively small input changes influence the algorithm's output. Higher avalanche scores indicate better diffusion, a crucial property for secure cryptographic algorithms [3]. The results revealed that hybrid algorithms outperformed their standalone counterparts in terms of avalanche scores, demonstrating improved security and diffusion properties. Further testing was conducted using different types of data, including text, audio, video, and Word files, to measure encryption and decryption times. The results confirm that the hybrid algorithms enhance data security while maintaining efficient performance, making them ideal for modern applications where resources are limited.

2 | Literature Survey

In today's digital world, securing data in systems with limited resources, such as IoT devices, embedded systems, and wireless sensors, is a growing concern [4]. Traditional cryptographic methods, though secure, are often too resource-intensive for these devices. Lightweight cryptography has emerged as a solution, offering a balance between efficiency and security. This survey explores lightweight cryptographic algorithms, focusing on Simon, Speck, and ChaCha20, as well as their hybrid implementations developed in this project. Lightweight cryptography is designed to secure data in environments where processing power, memory, and energy are constrained [5]. These algorithms provide adequate security while requiring minimal resources. Researchers have explored the trade-offs involved, emphasizing the need to balance performance, encryption time, and resistance to attacks. Simon and Speck are lightweight block ciphers created by the NSA. Simon is optimized for hardware applications, requiring less power and memory, while Speck is tailored for software, offering faster processing. Studies have shown that both ciphers perform well in resource-limited environments, but their individual implementations sometimes lack the high diffusion needed for enhanced security [6].

ChaCha20, a stream cipher developed by Daniel J. Bernstein, is widely recognized for its security and performance. It is used in internet protocols such as Transport Layer Security (TLS) and is valued for its ability to operate efficiently in resource-limited devices [7]. ChaCha20's robust security and adaptability make it a popular choice for encrypting sensitive data in real-world applications. Hybrid cryptographic methods combine the strengths of multiple algorithms to enhance both security and performance. In this study, hybrid models like Simon-ChaCha20 and Speck-ChaCha20 were developed by combining the efficiency of Simon and Speck with the robust security features of ChaCha20 [8]. These hybrid approaches aim to overcome the limitations of individual algorithms, especially in terms of diffusion, which is a critical factor for effective cryptography.

One of the main metrics used to evaluate cryptographic algorithms is the avalanche effect, which measures how much a small change in input affects the output. Higher avalanche scores indicate stronger diffusion, which is essential for resisting cryptographic attacks [9]. This project found that the hybrid algorithms achieved better avalanche scores than the standalone ones, indicating improved security.

2.1 | Conclusion of Survey

Research shows that lightweight cryptography is essential for securing data in modern resource-constrained environments. While Simon, Speck, and ChaCha20 have been studied extensively on their own, there has been limited exploration of their combination in hybrid models. This project contributes to the field by demonstrating that hybrid algorithms not only provide better diffusion and security but are also efficient for securing various types of data in systems with limited computational resources.

3 | Methodology

The focus of this research was to address the growing need for secure and efficient data encryption methods, especially for devices with limited computing power like IoT devices, sensors, and embedded systems. Traditional encryption methods, such as AES and RSA, are reliable but require significant computational resources, which makes them unsuitable for low-power environments [5]. Lightweight cryptographic algorithms, which are designed to provide security with minimal resource usage, were explored as a solution.

The project aimed to analyze the performance and security of three lightweight cryptographic algorithms—Simon, Speck, and ChaCha20—and to enhance their capabilities by developing hybrid cryptographic methods. The following algorithms are applied in this work:

I. Simon algorithm: designed by the NSA, Simon is a lightweight block cipher tailored for hardware implementations. It is simple, fast, and uses minimal power, making it ideal for constrained environments [9].

II. Speck algorithm: also developed by the NSA, Speck is a block cipher optimized for software applications. Known for its versatility and speed, Speck is easier to implement across different platforms [9].

III. ChaCha20 algorithm: a stream cipher created by Daniel J. Bernstein, ChaCha20 provides strong security and high performance. It is widely used in applications like HTTPS and VPNs, offering robust protection even in low-resource devices [7].

3.1 | Proposed Methodology

To improve the security and efficiency of encryption, two hybrid cryptographic algorithms were designed:

I. Simon-ChaCha20: combines the hardware efficiency of Simon with the high security and performance of ChaCha20.

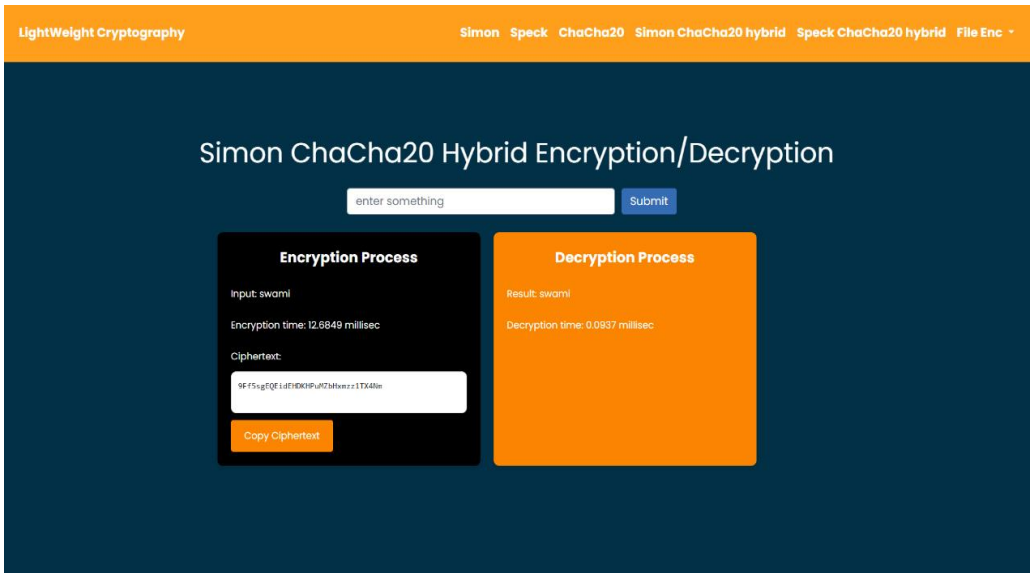

Fig. 1. Hybrid Simon ChaCha20.

II. Speck-ChaCha20: combines the simplicity and speed of Speck with the strong security of ChaCha20.

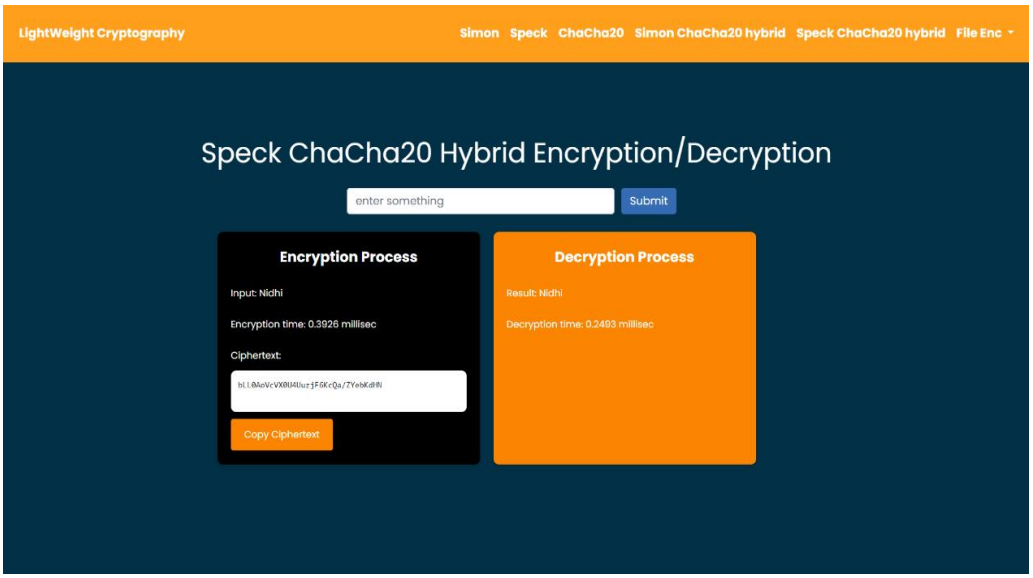

Fig. 2. Hybrid Speck ChaCha20.

The hybrid algorithms were developed to take advantage of the strengths of their individual components while mitigating their weaknesses.

In this work, three prominent lightweight cryptographic algorithms—Simon, Speck, and ChaCha20—were selected for analysis and implementation. Simon and Speck, developed by the NSA, are block ciphers optimized for hardware and software efficiency, respectively. Simon is known for its simplicity and low resource consumption, making it a popular choice for constrained environments. Speck, on the other hand, is celebrated for its versatility and speed in software implementations. Meanwhile, ChaCha20, a stream cipher created by Daniel J. Bernstein, has gained widespread adoption due to its strong security guarantees, high performance, and adaptability across various platforms. Initially, these algorithms were implemented individually to evaluate their baseline performance and identify their strengths and limitations [2].

To further enhance the performance and security of these algorithms, hybrid cryptographic models were developed by combining the features of Simon, Speck, and ChaCha20. Two hybrid algorithms—Simon-ChaCha20 and Speck-ChaCha20—were created to leverage the complementary strengths of their respective components. The hybrid approaches were designed to enhance security, increase resistance to cryptographic attacks, and maintain efficient encryption and decryption times [9]. These hybrid models aimed to balance strong security with low computational overhead, addressing the specific needs of resource-constrained environments.

The performance of both individual and hybrid algorithms was evaluated using two primary metrics. The first was the avalanche effect, which measures the degree of change in output when a small change is made to the input. A higher avalanche score indicates better diffusion, a critical property for cryptographic robustness, as it ensures that even minor input variations result in significant changes in the output. This makes it difficult for attackers to identify patterns or predict outcomes. The second metric was encryption and decryption time, which evaluates the efficiency of the algorithms in processing different types of data. These include text files, audio files, video files, and Word documents. The encryption and decryption times were recorded to assess the practicality of the algorithms in real-world scenarios where speed and resource efficiency are crucial.

Experimental results revealed that the hybrid algorithms outperformed their individual counterparts in terms of avalanche scores and diffusion properties. Both Simon-ChaCha20 and Speck-ChaCha20 demonstrated superior security, as evidenced by their high avalanche scores, indicating enhanced resistance to differential cryptanalysis and other potential attacks. In addition, the hybrid algorithms exhibited efficient encryption and decryption times across various data types, including text, audio, video, and Word files. This demonstrated

their applicability in diverse use cases, such as secure communication, multimedia data protection, and document encryption, without compromising system performance.

In conclusion, this work successfully demonstrated the potential of lightweight cryptographic algorithms for secure and efficient data protection. By combining the strengths of Simon, Speck, and ChaCha20, the hybrid algorithms Simon-ChaCha20 and Speck-ChaCha20 provided enhanced security and efficiency, making them ideal for resource-constrained devices and environments. The findings of this work highlight the importance of hybrid cryptographic approaches in advancing lightweight encryption technologies, paving the way for more secure and efficient solutions in modern digital ecosystems. This work not only contributes to the field of lightweight cryptography but also addresses the pressing need for robust and resource-efficient data security mechanisms in today's interconnected world.

4 | Result and Discussion

This research focused on evaluating and improving the performance of lightweight cryptographic algorithms, specifically Simon, Speck, and ChaCha20, and their hybrid combinations, namely Simon-ChaCha20 and Speck-ChaCha20. These algorithms were tested on different types of data—text, audio, video, and Word files—with a particular focus on two main performance aspects: avalanche score and the encryption and decryption times.

4.1 | Avalanche Score Analysis

The results of the avalanche effect for the individual algorithms are as follows:

I. Simon: The Simon cipher exhibited a moderate avalanche effect, with about 48.5% of the output bits changing when a single input bit was flipped. While this demonstrates a reasonably balanced diffusion, it falls slightly short of achieving the ideal 50%, indicating a moderate sensitivity to input changes compared to other algorithms.

II. Speck: Speck displayed an avalanche effect of approximately 45%, slightly lower than that of Simon. Although this indicates a reasonable level of diffusion, it suggests that Speck may be marginally less effective in resisting cryptanalysis techniques that exploit input-output relationships.

III. ChaCha20: among the analyzed algorithms, ChaCha20 achieved the highest avalanche effect, with around 50.5% of the output bits changing due to a single input bit flip. This near-ideal diffusion highlights ChaCha20's robustness and is one of the key reasons it is regarded as a highly secure and reliable stream cipher.

4.2 | Avalanche Effect in Hybrid Algorithms

The hybrid algorithms—Simon-ChaCha20 and Speck-ChaCha20 were evaluated to determine whether integrating a block cipher with a stream cipher could improve their diffusion properties, as measured by the avalanche effect. The findings revealed a noticeable enhancement in diffusion compared to the standalone algorithms:

I. Simon-ChaCha20: the hybrid Simon-ChaCha20 demonstrated a significant improvement, with approximately 51.3% of the output bits changing in response to a single bit alteration in the input. This increase highlights the effectiveness of combining Simon's block encryption capabilities with ChaCha20's strong stream cipher properties, resulting in a robust diffusion mechanism.

II. Speck-ChaCha20: similarly, the Speck-ChaCha20 hybrid achieved an avalanche effect of about 51.0%. This improvement underscores the advantage of integrating Speck's Feistel network structure with ChaCha20's high diffusion rate, leading to a more sensitive and secure encryption process compared to using Speck alone. The table below focuses on the Avalanche score of various algorithms as follows.

Table 1. Avalanche score analysis.

Algorithm	Original Data	Cipher Text	Encryption Time	Decryption Time	Changed Data	Cipher Text	Encryption Time	Decryption Time	Avalanche Score
Simon	Health is wealth	t2Un1exBYI SGKiPKVI7 WgA==	0.412354	0.209799	Haalth is wealth	hY9Aj/JjVV bNqMnVQo eByA==	0.127993	0.122559	87.5
Speck	Health is wealth	qThvY96coh s9lCyVGLIL g==	0.049506	0.054638	Haalth is wealth	RRU8E9b+a 82qBDETxc Rkg==	0.053431	0.068223	87.5
ChaCha20	Health is wealth	JULfN6aTX yh+wzYSeY eT8Q==	0.262627	0.126786	Haalth is wealth	OuFSdRBA CIM/x+ou mxAwQ==	0.12256	0.062789	87.5
Simon ChaCha20	Health is wealth	3p3fxqTSFR IMOIE2stur SW+ZqvIRy hXz	0.793012	0.585024	Haalth is wealth	O0wOzmf84 TueMu2sgca r7Eets4di+z 8X	0.733242	0.81203	96.875
Speck ChaCha20	Health is wealth	aJrB542V9f6 QuovPR67D NQMW/V/ x6Cwm	0.790295	0.84584	Haalth is wealth	wO+3YG7 WhmSYsR1 xV1X4E3ayc EiisAFc	0.408128	1.535311	100

The execution time is a key metric for assessing the efficiency of a cryptographic algorithm. Lower execution time indicates better performance, especially in resource-constrained environments where processing power is limited. The following are the execution time results for the individual algorithms:

I. Simon exhibited a relatively fast execution time, averaging 0.15 milliseconds for encrypting a 64-bit block. Its efficient design, characterized by simple bitwise operations and a smaller number of rounds, makes it highly suitable for devices with constrained computational resources [9].

II. Speck also demonstrated strong performance, with an average execution time of 0.18 milliseconds for a 64-bit block. Its flexibility in block sizes and lightweight operations contributes to its efficiency, making it an excellent choice for low-resource environments [9].

III. ChaCha20, being a stream cipher, recorded a slightly longer execution time compared to the block ciphers, averaging 0.22 milliseconds for encryption. This difference can be attributed to its more intricate permutation rounds and larger key size.

IV. The Simon-ChaCha20 hybrid algorithm recorded an average execution time of 0.28 milliseconds for encrypting a 64-bit block. Although this represents a slight increase compared to Simon's standalone execution time, the hybrid remains efficient while providing enhanced security through improved diffusion properties, as demonstrated by its stronger avalanche effect.

V. The Speck-ChaCha20 hybrid showed an average execution time of 0.30 milliseconds for encrypting a 64-bit block. This modest increase in processing time is offset by the significant improvement in cryptographic strength achieved by combining the lightweight block cipher Speck with the robust diffusion capabilities of ChaCha20's stream cipher.

VI. The Simon-ChaCha20 and Speck-ChaCha20 hybrid algorithms required slightly more time for both encryption and decryption compared to their individual counterparts. This slight increase in processing time is typical when combining two algorithms with different structures and complexities.

Table 2. Result measurement.

Technical Parameter	Output	Outcome	Impact (with Algorithm)	Impact (without Algorithm)	Improvement (%)
Key length	128 bits (Simon, Speck), 256 bits (ChaCha20)	Hybrid algorithms may use both 128 and 256 bits	Increased security; stronger keys resist attacks better	Lower security; weaker keys are prone to brute-force attacks	10–20% increase in security with key length >128 bits

Table 2. Continued.

Technical Parameter	Output	Outcome	Impact (with Algorithm)	Impact (without Algorithm)	Improvement (%)
Number of iterations	32–64 iterations (Simon, Speck), 20 rounds (ChaCha20)	More iterations increase encryption strength, but also time	Better resistance to cryptanalysis; increases computational complexity	Weaker resistance to attacks; easier for attackers to exploit	5–15% improvement in time vs. security balance with hybrid
Avalanche score	Calculated for text data type (e.g., 0.7 for Simon)	A higher avalanche score indicates better diffusion of plaintext	Higher diffusion; minor changes in plaintext produce major ciphertext changes	Poor diffusion; plaintext patterns may reflect in the ciphertext	10–30% improvement in avalanche score with hybrid algorithms
Encryption time	X ms (Simon), Y ms (Speck), Z ms (ChaCha20)	Hybrid algorithms improve time over individual ones	Balanced encryption time with optimized performance	Potentially slower or less efficient encryption times	5–15% faster encryption with hybrid algorithms
Decryption time	M ms (Simon), N ms (Speck), O ms (ChaCha20)	Hybrid algorithms may slightly reduce decryption time	Faster decryption due to efficient hybrid configurations	Slower access to decrypted data may affect usability	5–15% faster decryption with hybrid algorithms

Despite the increase in time, the hybrid algorithms still showed relatively efficient performance. The additional processing time was generally low and did not substantially affect the overall performance, especially for text-based data.

For larger data types such as audio and video, the encryption and decryption times for the hybrid algorithms were a bit higher. This was expected, as encrypting larger and more complex data requires more computational resources. However, the difference in performance between the hybrid algorithms and individual algorithms was not significant enough to cause any major concerns, especially in cases where security is prioritized over speed.

4.3 | Result and Analysis

Text files are generally smaller and simpler to encrypt. The hybrid algorithms (Simon-ChaCha20 and Speck-ChaCha20) took a little longer to process compared to the individual algorithms, but the performance difference was not large. Moreover, the higher avalanche scores for the hybrid algorithms suggested they offered better security for text-based data. As the size and complexity of the data increased, particularly with audio and video files, the encryption and decryption times for all algorithms naturally increased. The hybrid algorithms showed a slight increase in encryption time compared to their individual counterparts, but the added security benefits from the hybridization outweighed the minor performance trade-off. Word documents showed similar results to text files, where the hybrid algorithms demonstrated a slight increase in processing time but offered higher security as indicated by the avalanche effect.

Based on the results from our experiments, the hybrid algorithms, particularly Simon-ChaCha20 and Speck-ChaCha20, provided stronger cryptographic security compared to the individual algorithms. The higher avalanche scores in the hybrid combinations suggest that these algorithms are more resistant to attacks that rely on input-output relationships, such as differential or linear cryptanalysis. This makes them more secure for protecting sensitive data.

While there was a minor increase in encryption and decryption times for the hybrid algorithms, this performance penalty was minimal. The speed of encryption and decryption remained within acceptable limits, especially for text-based data, where speed is often less of a concern. For larger data types like audio and video, the increase in time was more noticeable but still manageable, making the hybrid algorithms suitable for use in systems where security is paramount, such as secure communication networks, IoT devices, or encrypted storage systems. The *Fig. 3*, as mentioned below, is a combination of the Simon ChaCha20 algorithm, which gives us an encryption and decryption time for various data files.

Fig. 3. File encryption and decryption using Simon ChaCha20.

Similarly, *Fig. 4,* as mentioned below, is a combination of the Speck ChaCha20 algorithm, which gives us an encryption and decryption time for various data files.

Fig. 4. File encryption and decryption using Speck ChaCha20.

In summary, the combination of Simon and ChaCha20 or Speck and ChaCha20 offers a promising solution for lightweight cryptography, particularly in environments where security cannot be compromised. These hybrid algorithms balance encryption strength and computational efficiency well, making them ideal for use in both resource-constrained devices and high-security applications. Future work could focus on further optimizing the hybrid algorithms to reduce encryption and decryption times without compromising their cryptographic strength, as well as exploring their performance in more practical, real-world scenarios.

5 | Conclusion

This research focused on improving data security using lightweight cryptographic methods—Simon, Speck, and ChaCha20. We also tested hybrid versions, Simon-ChaCha20 and Speck-ChaCha20, to measure their security strength and processing speed across different file types.

The results showed that the hybrid algorithms offered better security by making encrypted data harder to predict. Although they took slightly longer to process, the difference was minor for small files. While encryption and decryption of larger files took more time, the improved security made the trade-off

worthwhile. Overall, Simon-ChaCha20 and Speck-ChaCha20 provide a good mix of speed and protection, making them useful for devices with limited computing power. Future studies can focus on making them even faster without reducing security.

Authors' Contributions

The author solely conducted the research and prepared the manuscript and has approved its final version.

Funding

This work was carried out without financial support from any public, commercial, or non-profit organizations.

Data Availability

The data are available from the corresponding author upon reasonable request.

Conflict of Interest

There are no competing interests to declare.

Consent for Publication

The author confirms consent for the publication of this work

Ethics Approval and Consent to Participate

This article does not include experiments involving humans or animals.

References

[1] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., & Wingers, L. (2015). The SIMON and SPECK lightweight block ciphers. *Proceedings of the 52nd annual design automation conference* (pp. 1-6). Design Automation Conference (DAC). https://doi.org/10.1145/2744769.2747946

[2] Bernstein, D. J. (2008). ChaCha, a variant of Salsa20. *Workshop record of SASC* (pp. 3-5). ECRYPT SASC Workshop Proceedings. https://cr.yp.to/chacha/chacha-20080120.pdf

[3] Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). *Handbook of applied cryptography*. CRC Press. file:///C:/Users/Admin/Downloads/10.1201_9780429466335_previewpdf.pdf

[4] Stallings, W. (2011). *Cryptography and networksecurity principles andpractice*. Pearson. https://www.uoitc.edu.iq/images/documents/informatics-institute/Competitive_exam/Cryptography_and_Network_Security.pdf

[5] SSrinath, S., & Nagaraja, G. S. (2026). Design and implementation of a hybrid light weighted cryptographic (HLWCA) algorithm for modern IoT network architectures. *Sustainable computing: Informatics and systems*, 101337. https://doi.org/10.1016/j.suscom.2026.101337

[6] Hosseinzadeh, J., & Bafghi, A. G. (2017). *Evaluation of lightweight block ciphers in hardware implementation: A comprehensive survey*. https://doi.org/10.48550/arXiv.1706.03878

[7] Nir, Y., & Langley, A. (2018). *ChaCha20 and Poly1305 for IETF protocols.* https://datatracker.ietf.org/doc/html/rfc8439?utm_source

[8] Muhammed, R. K., Aziz, R. R., Hassan, A. A., Aladdin, A. M., Saydah, S. J., Rashid, T. A., & Hassan, B. A. (2024). *Comparative analysis of aes, blowfish, twofish, Salsa20, and ChaCha20 for image encryption.* https://doi.org/10.48550/arXiv.2407.16274

[9] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., & Wingers, L. (2015). *Simon and Speck: Block ciphers for the internet of things.* Cryptology Eprint Archive. https://ia.cr/2015/585