EasyChair Preprint

№ 13715

Trend Analysis and Statistical Cryptoanalysis of Light Weight Block Ciphers

Sajal Fayyaz

July 1, 2024

Trend Analysis and Statistical Cryptoanalysis of Light weight Block ciphers

Sajal Fayyaz
D*ept of Computer Science*
Sir Syed College of Computer Science
Affiliated with University of
Engineering and Technology ,Lahore
Lahore, Pakistan
sajalfayyaz9@gmail.com

***Abstract*—Lightweight block ciphers have become essential for securing data in Iot devices and other resource-constrained environments. Encryption serves as a vital method for ensuring information security, yet a deeper analysis of the relationship between algorithm components and their security strength is needed. In this paper, we present a comprehensive systematic literature review of 101 existing lightweight block ciphers, focusing on their security aspects and the selection of secure design components, such as substitution and permutation functions.**

This review examines the evolution of lightweight algorithms and their performance in terms of RAM size and execution cycles. By exploring the impact of these design choices on security strength, we identify the importance of incorporating confusion and diffusion properties to develop robust algorithms. The findings provide recommendations for developers on designing secure algorithms, while highlighting modern advances and potential future research directions in the field.As technology advances rapidly, it is crucial to understand the challenges and solutions in lightweight cryptography. This knowledge will help develop stronger protection methods as crypt analysts continue to break ciphers once deemed unbreakable. Ultimately, this research aims to contribute to the ongoing development of effective security measures for emerging technologies.

Keywords—Lightweight, Small-Computing-Devices, Block-cipher (*key words****)***

I. INTRODUCTION

The Internet of Things (IoT) has emerged as a crucial technology across various industries, leveraging sensors, actuators, and monitors connected to the Internet for a wide array of applications. As technology advances, the demand for IoT applications has risen, leading to increased data exchanges between interconnected devices. Ensuring the security of these data exchanges is essential, particularly given the lightweight nature of many IoT devices such as sensors, RFID tags, and smartcards.

Traditional block cipher schemes like AES, designed for more robust computing environments, can be unsuitable for lightweight IoT devices due to their high operational overhead. In contrast, lightweight block ciphers offer a simpler, more resource-efficient alternative, featuring smaller block and key sizes tailored for constrained devices. These ciphers fulfill key properties such as providing moderate security despite attackers' limited data and computing capabilities, and being primarily implemented in hardware with some software components.

Lightweight block ciphers have become a standard for securing IoT devices, attracting significant interest from academia, industry, and government. Development of these algorithms dates back to the early 1990s with notable examples like IDEA, Blowfish, and TEA. Today, hundreds of lightweight algorithms have been proposed, drawing inspiration from existing algorithms like AES and PRESENT. These established ciphers continue to influence the design of new lightweight block ciphers.

Previous research has primarily focused on the performance and implementation of lightweight ciphers, while the relationship between design components and security strength has been largely overlooked. This research aims to fill that gap by analyzing how design choices impact the strength of lightweight block ciphers. Understanding the nuances of design, such as confusion and diffusion properties achieved through substitution and permutation, is crucial for developing secure and efficient algorithms for resource-constrained environments.

This paper presents an in-depth study of lightweight block ciphers, offering a detailed analysis of existing algorithms and their design components. We examine substitution and permutation functions to assess their impact on security strength and provide insights into the evolution of lightweight ciphers. By bridging the gap in existing research, this paper aims to guide developers in designing robust, secure, and efficient lightweight block ciphers for the ever-expanding Iot landscape.

The Internet of Things (IoT) has rapidly gained prominence as a critical technology across numerous sectors, including healthcare, manufacturing, transportation, and smart homes. IoT enables the connection of devices such as sensors, actuators, and monitors to the Internet, facilitating vast data exchanges across networks. This surge in connected devices necessitates strong security measures to protect data integrity and privacy.

Lightweight block ciphers have become a popular solution for securing data within IoT systems, as they offer a balance between security and the limited resources available in IoT devices. Conventional block cipher schemes like AES, designed for high-performance computing environments, may be too resource-intensive for lightweight devices, such as sensors, RFID tags, and smartcards. In response, lightweight block ciphers feature smaller block and key sizes, simpler operations, and minimal resource

consumption, making them suitable for resource-constrained environments.

The development of lightweight block ciphers began in the early 1990s with notable algorithms such as IDEA, Blowfish, and TEA. Since then, hundreds of lightweight algorithms have been proposed, including recent advances such as LBC-IoT, improved SM4, and LAO-3D. Many of these designs are influenced by existing algorithms like AES and PRESENT, reflecting the ongoing relevance of established cryptographic approaches in the lightweight cipher domain.

However, while research on lightweight block ciphers has focused extensively on performance and implementation aspects, there is a notable gap in understanding the relationship between design components and security strength. This research paper seeks to address this gap by conducting an in-depth study of lightweight block ciphers, emphasizing the importance of confusion and diffusion properties, achieved through substitution and permutation components, in ensuring robust security.

We examine 101 lightweight algorithms to analyze their substitution and permutation functions, assessing their impact on the security strength of these ciphers. This study delves into the key design aspects that contribute to the effectiveness of lightweight block ciphers in securing IoT systems. By exploring the evolution of these algorithms, including encryption and key schedule components, we provide insights into the development of future secure and efficient lightweight ciphers.

Embedded Systems are utilized across diverse sectors such as industrial installations, critical environments, mobile setups, private domains, and public infrastructures. Their functionality typically encompasses the handling of sensitive or critical data, necessitating robust security measures to safeguard their resources and services. Consequently, there is a growing demand for cryptographic components suitable for these systems. However, the constraints of embedded devices, including limited resources, compact size requirements, and cost considerations, pose challenges for deploying traditional secure algorithms.

II. Lightweight block ciphers : an overview

Lightweight block ciphers are specifically designed for resource-constrained environments, offering compact implementations with small key and block sizes. They prioritize efficiency and low computational overhead while maintaining adequate security levels for constrained devices.In the era of IoT and ubiquitous computing, lightweight block ciphers play a crucial role in securing communication between constrained devices. Their efficiency and small footprint make them ideal for applications where computational resources are limited, such as smartcards, sensor networks, and RFID systems.
Lightweight block ciphers find widespread use in various IoT applications, including secure data transmission, device authentication, and access control. Their compact design makes them suitable for embedding in microcontrollers and other low-power devices, enabling secure communication in IoT ecosystems.

III. Key Lightweight block ciphers

A. *PRESENT*

PRESENT stands out in the realm of lightweight block ciphers due to its simplicity and efficiency. With a 64-bit block size and a variable key size, it's tailored for resource-constrained devices without compromising on security. Its compact design makes it particularly suitable for applications where memory and processing power are limited. Despite its simplicity, PRESENT offers robust cryptographic protection, making it a popular choice for various constrained environments. Its flexibility in key size adds another layer of adaptability, allowing it to be fine-tuned based on specific security requirements. Overall, PRESENT serves as a prime example of a lightweight cipher that strikes a balance between simplicity, efficiency, and security, making it a go-to option for securing IoT devices, smart cards, and other embedded systems.

B. *SPECK AND SIMON*

SPECK and SIMON, developed by the NSA, form a formidable family of lightweight block ciphers that excel in both performance and security. These ciphers are optimized for small key and block sizes, catering specifically to the needs of IoT applications. Their efficient designs ensure minimal computational overhead, making them ideal for resource-constrained devices with limited processing capabilities. Despite their compact nature, SPECK and SIMON boast impressive cryptographic strength, providing a robust defense against various attacks. Their versatility and high performance have cemented their status as go-to choices for securing IoT networks, sensor nodes, and other constrained environments. With ongoing scrutiny and analysis, these ciphers continue to demonstrate resilience and adaptability, remaining at the forefront of lightweight cryptography.

C. *KATAN AND KTANTAN*

KATAN and KTANTAN represent a class of lightweight block ciphers finely tuned for hardware implementation. These ciphers feature small key and block sizes, optimized to minimize hardware requirements and energy consumption. Their streamlined architectures make them well-suited for integration into low-power devices commonly found in IoT and RFID systems. Despite their compact footprint, KATAN and KTANTAN offer robust security features, ensuring the confidentiality and integrity of transmitted data. Their efficiency in hardware makes them an attractive choice for applications where energy efficiency and performance are paramount. As the demand for lightweight cryptography continues to rise, KATAN and KTANTAN stand as reliable solutions for securing a wide range of resource-constrained devices, from wearable electronics to industrial sensors.

IV. DESIGN PRINCIPLES OF LIGHTWEIGHT BLOCK CIPHERS

Design principles in lightweight block ciphers dictate the delicate balance between security and efficiency. Key and block sizes, rounds, S-boxes, and P-boxes are meticulously calibrated to thwart attacks while minimizing computational overhead. Achieving this equilibrium ensures robust cryptographic protection in resource-constrained environments.

A. Key Size and Key Block Consideration

In lightweight block ciphers, the selection of key and block sizes is pivotal, striking a delicate balance between security and efficiency. While smaller key and block sizes alleviate computational burdens, they also shrink security margins, potentially rendering the cipher vulnerable to attacks. Therefore, designers must meticulously calibrate these sizes to ensure robust cryptographic protection without unduly burdening constrained devices.

B. Rounds and Round Function

The number of rounds and the intricacies of the round function profoundly influence the security posture of lightweight block ciphers. Determining the optimal number of rounds necessitates a nuanced understanding of cryptographic principles, ensuring adequate security while maintaining acceptable performance levels. Balancing these factors is crucial to thwarting potential attacks and fortifying the cipher's resilience.

C. S-Boxes and P-Boxes

Substitution-boxes (S-boxes) and permutation-boxes (P-boxes) are integral to the design of lightweight block ciphers, imbuing them with essential confusion and diffusion properties. The efficacy of these components directly impacts the cipher's resistance to cryptanalysis, shaping its overall security robustness. Careful consideration and meticulous design of S-boxes and P-boxes are imperative to bolstering the cipher's defensive capabilities against adversarial threats.

D. Performance vs Security Tradeoff

In the realm of lightweight block cipher design, navigating the intricate trade-offs between performance and security is paramount. While optimizing for one facet may yield gains, it often necessitates concessions in the other, necessitating a judicious equilibrium. Striking this balance requires a comprehensive understanding of application requirements and threat landscapes, ensuring that the cipher's design effectively mitigates potential risks while delivering optimal performance in resource-constrained environments.

V. CHALLENGES IN SECURING LIGHTWEIGHT BLOCK CIPHERS

Securing lightweight block ciphers is a complex challenge that spans cryptography, computer science, and engineering, necessitated by the need to balance security, efficiency, and resource constraints. This balance is critical for ensuring the continued security and functionality of lightweight block ciphers amidst evolving threats and technological progress.

One of the primary challenges is maintaining the delicate equilibrium between security and efficiency. Lightweight block ciphers are designed for resource-constrained devices, such as IoT sensors, smart cards, and RFID tags, which possess limited computational power and memory. These ciphers must prioritize efficiency to ensure optimal performance on such devices. However, enhancing efficiency often compromises security, as reductions in key sizes, block sizes, or the number of rounds can weaken cryptographic properties and increase vulnerability to attacks. Achieving this balance requires careful consideration of the specific application's security needs, performance requirements, and threat model.

Addressing specific attack vulnerabilities poses another significant challenge. The simplified design and reduced complexity of lightweight ciphers can render them susceptible to various cryptographic attacks, such as differential and linear cryptanalysis, and algebraic attacks. These attacks can allow adversaries to recover plaintext or secret keys, compromising the confidentiality and integrity of encrypted data. Mitigating these vulnerabilities demands thorough cryptanalysis to identify weaknesses and develop countermeasures to fortify security. Ongoing research is essential to anticipate and counteract emerging threats, including side-channel and fault attacks, which exploit implementation-specific weaknesses rather than intrinsic cryptographic flaws.

Implementing effective countermeasures is crucial to mitigating potential threats to lightweight block ciphers. Countermeasures might include additional security features such as key whitening, non-linear key scheduling, and lightweight authentication mechanisms to bolster resistance against attacks. Secure implementation practices, like randomizing memory access patterns and protecting sensitive data during cryptographic operations, can help mitigate the risks of side-channel and fault attacks. However, incorporating these countermeasures in resource-constrained devices introduces further challenges, as they must balance security, performance, and resource utilization.

Future research must address these challenges to ensure the ongoing security of lightweight block ciphers amidst evolving threats and technological advancements. This involves developing new cryptographic primitives and design techniques tailored to the unique demands of resource-constrained environments, as well as enhancing existing lightweight ciphers to withstand emerging attacks. Collaboration among researchers, industry stakeholders, and standards bodies is vital to promoting the widespread adoption of secure lightweight cryptographic algorithms and ensuring interoperability across diverse platforms and applications. By addressing these challenges collectively, the security and resilience of lightweight block ciphers can be enhanced, enabling their continued use in securing critical systems and applications in the digital era.

VI. MOTIVATION

In today's interconnected world, where information is transmitted and shared across vast networks, ensuring the confidentiality, integrity, and authenticity of data is paramount. Cryptography provides the means to achieve these objectives by employing various cryptographic techniques and algorithms. From encrypting sensitive communications to securing digital transactions, cryptography plays a vital role in safeguarding information from unauthorized access and manipulation.

Moreover, cryptography has a rich history dating back centuries, with its roots deeply intertwined with the evolution of human civilization. From ancient civilizations' use of simple substitution ciphers to the development of complex cryptographic algorithms in the modern era, cryptography has continuously evolved in response to new challenges and advancements in technology. Today, cryptographic techniques underpin the security of countless applications and systems, including online banking, e-commerce, secure messaging, and data storage.

As the digital landscape continues to evolve and new technologies emerge, the importance of cryptography in ensuring cybersecurity and privacy will only increase. Innovations in areas such as quantum computing, artificial intelligence, and the Internet of Things (IoT) present both opportunities and challenges for cryptography. Researchers and practitioners in the field must remain vigilant, continually advancing cryptographic techniques to stay ahead of adversaries and protect against emerging threats.

VII. LITERATURE REVIEW

This research paper provides a comprehensive literature review on lightweight block ciphers and their application in securing IoT devices. It analyzes previous studies to highlight key insights, trends, and gaps, focusing on the design, performance, and security implications of lightweight block ciphers for IoT systems. These ciphers are tailored to the constraints of IoT devices, offering various block and key sizes and operational approaches.

The review assesses notable lightweight block ciphers such as LBC-IoT, improved SM4, and LAO-3D, discussing their unique design features and potential for secure IoT applications. Previous research has extensively explored the performance and implementation of lightweight ciphers in resource-constrained environments, examining optimization techniques to enhance efficiency across different hardware and software platforms. However, there is a notable gap regarding the relationship between design components and security strength in these ciphers.

This paper aims to fill this gap by analyzing 101 lightweight algorithms, focusing on substitution and permutation functions and their impact on security strength. It delves into key schedule components and encryption mechanisms, providing insights into the evolution and development of future lightweight ciphers that balance security with efficiency.

The review underscores the ongoing relevance of established cryptographic approaches in the lightweight cipher domain and highlights the need for further research into the security aspects of lightweight block ciphers, particularly for IoT applications. By understanding the nuances of design choices and their security outcomes, this paper seeks to guide developers in creating robust and efficient lightweight block ciphers for IoT systems.

The study reveals various methods for creating secure encryption algorithms, emphasizing the effectiveness of combining substitution and permutation techniques to achieve essential confusion and diffusion properties. Current trends indicate a shift towards lightweight ciphers with a single 4-bit S-box, 128-bit or smaller keys, and over 20 rounds of encryption. These trends aim to strike a balance between security and efficiency, equipping researchers with knowledge for designing secure lightweight ciphers and emphasizing the need for further exploration to counter evolving cyber threats on resource-constrained devices.

VIII. RESEARCH FRAMEWORK

This discussion examines the ethical dimensions of security and privacy in computer and information technology, particularly focusing on electronic medical records (EMRs). It begins by exploring foundational ethics, emphasizing consequentialism and deontology as frameworks for moral reasoning in information security. The burgeoning field of computer ethics is then addressed, highlighting the responsibilities of professionals and users and the ethical dilemmas in public policy concerning IT.

The text delves into system and information security's importance in safeguarding digital assets, addressing the moral imperative of protecting digital infrastructure and the intricate relationship between computer and national security. It considers the ethical implications of security research, especially regarding privacy and power dynamics.

Critical theory is introduced as a lens to examine EMR security ethics, proposing an empirical study to analyze information systems security policies in healthcare. This study aims to understand the practical implementation of security measures in EMRs and their ethical concerns.

The broader implications for technology ethics and governance are discussed, with an emphasis on integrating critical theory to explore nuanced ethical considerations in EMR security. The analysis focuses on power dynamics, ownership issues, and the challenges of translating strategic policies into concrete measures.

IX. METHODOLOGY

The research methodology for the study on lightweight block ciphers involves several components. The scope of the study includes examining 101 lightweight block cipher algorithms, focusing on their design components such as substitution and permutation functions. The goal is to explore the relationship between these design choices and the security strength of the ciphers, including established

algorithms like IDEA, Blowfish, TEA, AES, and PRESENT, as well as newer ciphers such as LBC-IoT, improved SM4, and LAO-3D. A comprehensive review of existing research on lightweight block ciphers will be conducted, focusing on performance and implementation aspects.
This review will identify any gaps in current literature, particularly regarding the relationship between design components and security strength. Each of the 101 lightweight block cipher algorithms will be examined in detail. The analysis will involve assessing the design components, such as substitution and permutation functions, key schedule components, and other structural features.
The impact of these design choices on overall security strength and efficiency of the algorithms will be evaluated. Data on design aspects and performance metrics of each cipher will be collected, such as key size, block size, and operational overhead. Known vulnerabilities or weaknesses associated with each cipher, as well as their usage in various IoT applications, will be gathered. Criteria for evaluating the security and efficiency of the ciphers will be defined, including resistance to known attacks, resource consumption, and operational complexity.
Benchmarks or standards based on existing cryptographic approaches and industry best practices will be established. Quantitative and qualitative methods will be used to assess the impact of design choices on the security and performance of the algorithms. Cryptanalysis and simulations will be performed to test the ciphers' resistance to various attacks. Performance and security of different algorithms will be compared using statistical and analytical techniques. Findings from the analysis will be interpreted in terms of their implications for IoT security and lightweight cipher design.
The results will be discussed in relation to the existing literature and the broader context of IoT security. Recommendations for the design of robust, secure, and efficient lightweight block ciphers will be provided. The key findings and contributions of the study will be summarized. Areas for future research based on the outcomes and any limitations identified during the study will be suggested. This methodology aims to provide a comprehensive analysis of lightweight block ciphers and offer valuable insights into their design, security, and efficiency for securing IoT systems.

X. FUTURE RESEARCH

The conclusion of this research paper emphasizes the critical role of lightweight block ciphers in the rapidly expanding Internet of Things (IoT). Through a comprehensive analysis of 101 lightweight algorithms, the study highlights how specific design choices impact the security strength and efficiency of these ciphers, with a particular focus on the substitution and permutation functions that ensure robust confusion and diffusion properties.

Key insights from the analysis guide the development of more secure and efficient lightweight block ciphers tailored to IoT applications. The research acknowledges the continued relevance of established cryptographic methods, which provide a foundation for future innovations in lightweight cryptography. The paper stresses the need for ongoing research to deepen the understanding of the complex relationship between design decisions and cryptographic security. By contributing to this area, the study supports the advancement of robust cryptographic solutions essential for securing the increasing number of interconnected IoT devices.

The future of symmetric cryptography is poised for significant advancements driven by emerging technologies and evolving security needs. Key trends include the development of new algorithms that enhance security and efficiency. Researchers are continually exploring novel cryptographic techniques to provide stronger protection against advanced attacks while maintaining high performance.

Quantum computing poses a substantial threat to current cryptographic systems, including symmetric encryption, by potentially breaking traditional encryption methods. To counter this, the cryptographic community is exploring quantum-resistant algorithms designed to ensure robust security even with powerful quantum computers. Additionally, advancements in hardware technology, such as dedicated encryption hardware in secure enclaves and trusted execution environments, are enhancing the efficiency and security of encryption processes.

Machine learning and artificial intelligence (AI) are emerging as powerful tools in cryptography. AI can optimize encryption algorithms, detect vulnerabilities, and enhance key management processes, improving the overall resilience of encryption systems. Blockchain technology is also influencing symmetric cryptography, particularly in key management. Blockchain’s decentralized and immutable nature provides a secure framework for managing cryptographic keys, enhancing key distribution and revocation processes.

Homomorphic encryption, traditionally associated with asymmetric cryptography, is becoming feasible for integration with symmetric encryption, offering enhanced privacy and security for data processing in cloud environments. The rise of edge computing drives the need for more efficient and secure symmetric encryption techniques, ensuring data security in transit and at rest on edge devices without compromising performance.

Regulatory and compliance requirements continue to evolve, pushing the adoption of advanced encryption standards to protect sensitive data. User-friendly encryption solutions are gaining traction, making encryption more accessible to non-experts and ensuring broader adoption of robust data protection measures.

Collaborative efforts between academia, industry, and government agencies are crucial in shaping the future of symmetric cryptography. These collaborations facilitate the development of innovative cryptographic techniques and standards, ensuring that symmetric encryption evolves to meet emerging threats and technological advancements. In summary, the future of symmetric cryptography will be

driven by advancements in algorithm development, quantum computing resistance, hardware integration, AI, blockchain, homomorphic encryption, edge computing, regulatory influences, user-friendly solutions, and collaborative research, enhancing the security, efficiency, and scalability of symmetric encryption in the digital age.

XI. PROPOSED SOLUTION

The proposed solution detailed in the research paper involves a comprehensive approach to the design and analysis of lightweight block ciphers tailored for Internet of Things (IoT) applications. The paper focuses on enhancing the security of lightweight block ciphers while ensuring they remain efficient and resource-conscious for constrained IoT devices. The key components of the proposed solution include implementing confusion and diffusion principles in lightweight block ciphers using substitution and permutation components to achieve complexity in the cipher. This approach helps protect against attacks and maintain security. Optimized algorithms are recommended to strike a balance between performance and resource usage, ensuring that lightweight block ciphers can be effectively implemented in low-power and constrained devices.

The paper examines how design elements such as block and key sizes, substitution and permutation functions, and encryption and key schedule components contribute to the overall security strength of the ciphers. By balancing trade-offs between complexity and efficiency, the approach aims to maintain adequate security while adhering to resource constraints. The research provides a comparative analysis of 101 lightweight algorithms to identify the best-performing and most secure ciphers, considering factors such as computational overhead, security properties, and resistance to known attacks. Based on the evaluation, the paper offers specific recommendations for the adoption of certain lightweight block ciphers for specific IoT applications. Implementation strategies include adaptable solutions that work efficiently in both hardware and software contexts, as well as flexible key management strategies that optimize trade-offs between security and performance while accommodating diverse IoT use cases. The paper advocates for continued exploration and research into the interplay between design decisions and cryptographic security, which is critical to developing robust, efficient lightweight block ciphers that can adapt to the changing landscape of IoT security threats. Establishing standards and best practices in lightweight block cipher design can serve as guidelines for developers in the IoT field.

XII. CONCLUSION

The conclusion emphasizes the importance of lightweight block ciphers in the expanding IoT landscape, highlighting the critical impact of design choices on security strength and efficiency. Analyzing 101 lightweight algorithms, the study underscores the necessity of robust confusion and diffusion properties via substitution and permutation functions for effective lightweight ciphers. It demonstrates how established cryptographic approaches influence new, efficient designs, offering guidance for developers in creating secure IoT applications.

The research identifies current trends, noting that many lightweight block ciphers use a single 4-bit S-box, 128-bit or smaller keys, and over 20 encryption rounds. These trends are expected to continue to balance security and efficiency. The study advocates for ongoing exploration of lightweight cipher design, emphasizing security to counter sophisticated cyber-attacks. Future testing on diverse architectures and metrics is planned to ensure both performance and security standards are met.

REFERENCES

[1] Abd Al-Rahman, Seddiq Q., Sagheer, Ali Makki, Dawood, Omar A., 2018. NVLC: New variant lightweight cryptography algorithm for internet of things. In: Annual International Conference on Information and Sciences. IEEE, pp. 176–181.

[2] Aboshosha Bassam W., Dessouky Mohamed M., Ramdan Rabie A., El-Sayed, Ayman, 2019. LCA- Lightweight cryptographic algorithm for IoT constraint resources.

[3] In: International Conference on Electronic Engineering, pp. 374–380.

[4] Adams, Carlisle M., 1997a. Constructing symmetric ciphers using the CAST design procedure. Des. Codes, Cryptogr 12, 3, 283–316.

[5] Albrecht, Martin R., Driessen, Benedikt, Kavun, Elif Bilge, Leander, Gregor, Paar,

[6] Christof, Yalçın, Tolga, 2014. Block ciphers - Focus on the linear layer (feat PRIDE).

[7] Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I., & Manifavas, C. (2018). A review of lightweight block ciphers. Journal of cryptographic Engineering, 8, 141-184.

[8] Sehrawat, D., & Gill, N. S. (2018). Lightweight block ciphers for IoT based applications: a review. International Journal of Applied Engineering Research, 13(5), 2258-2270.

[9] Aboushosha, B., Ramadan, R. A., Dwivedi, A. D., El-Sayed, A., & Dessouky, M. M. (2020). SLIM: A lightweight block cipher for internet of health things. IEEE Access, 8, 203747-203757.

[10] Qassir, S. A., Gaata, M. T., & Sadiq, A. T. (2022). Modern and Lightweight Component-based Symmetric Cipher Algorithms. ARO-The Scientific Journal of Koya University, 10(2), 152-168.

[11] Abd Al-Rahman, Seddiq Q., Sagheer, Ali Makki, Dawood, Omar A., 2018. NVLC: New variant lightweight cryptography algorithm for internet of things. In: Annual International Conference on Information and Sciences. IEEE, pp. 176–181.

[12] Aboshosha Bassam W., Dessouky Mohamed M., Ramdan Rabie A., El-Sayed, Ayman, 2019. LCA- Lightweight cryptographic algorithm for IoT constraint resources.

[13] In: International Conference on Electronic Engineering, pp. 374–380.

[14] Adams, Carlisle M., 1997a. Constructing symmetric ciphers using the CAST designprocedure. Des. Codes, Cryptogr 12, 3, 283–316.

[15] Albrecht, Martin R., Driessen, Benedikt, Kavun, Elif Bilge, Leander, Gregor, Paar,Christof, Yalçın, Tolga, 2014. Block ciphers - Focus on the linear layer (feat PRIDE).

[16] In: Annual Cryptology Conference. Springer, Berlin, Heidelberg, pp. 57–76. Al-Dabbagh, Sufyan Salim Mahmood, 2017a. Design 32-bit lightweight block cipher algorithm (DLBCA). Int. J. Comput. Appl 166 (8), 17–20.

[17] Al-Dabbagh, Sufyan Salim Mahmood, Al-Shaikhli, Imad Fakhri Taha, 2013.

[18] Improving the security of LBlock lightweight algorithm using bit permutation.

[19] In: International Conference on Advanced Computer Science Applications and Technologies. IEEE, pp. 296–299.

[20] Al-Dabbagh, Sufyan Salim Mahmood, Al-Shaikhli, Imad Fakhri Taha, 2014. OLBCA: A new lightweight block cipher algorithm. In: International Conference on