electronics

MDPI

Article

Balancing Security and Efficiency: A Power Consumption Analysis of a Lightweight Block Cipher

Muhammad Rana *, Quazi Mamun * and Rafiqul Islam

School of Computing, Mathematics and Engineering, Charles Sturt University, Wagga, NSW 2678, Australia; mislam@csu.edu.au

* Correspondence: mrana@csu.edu.au (M.R.); qmamun@csu.edu.au (Q.M.)

Abstract: This research paper presents a detailed analysis of a lightweight block cipher's (LWBC) power consumption and security features, specifically designed for IoT applications. To accurately measure energy consumption during the execution of the LWBC algorithm, we utilised the Qoitech Otii Arc, a specialised tool for optimising energy usage. Our experimental setup involved using the Otii Arc as a power source for an Arduino NodeMCU V3, running the LWBC security algorithm. Our methodology focused on energy consumption analysis using the shunt resistor technique. Our findings reveal that the LWBC is highly efficient and provides an effective solution for energy-limited IoT devices. We also conducted a comparative analysis of the proposed cipher against established LWBCs, which demonstrated its superior performance in terms of energy consumption per bit. The proposed LWBC was evaluated based on various key dimensions such as power efficiency, key and block size, rounds, cipher architecture, gate area, ROM, latency, and throughput. The results of our analysis indicate that the proposed LWBC is a promising cryptographic solution for energy-conscious and resource-limited IoT applications.

Keywords: IoT security; power consumption; security trade-off; resource efficiency; lightweight block cipher

Citation: Rana, M.; Mamun, Q.; Islam, R. Balancing Security and Efficiency: A Power Consumption Analysis of a Lightweight Block Cipher. *Electronics* **2024**, *13*, 4325. https://doi.org/10.3390/electronics13214325

Academic Editors: Ping-Feng Pai, KiSung Park and Seungho Jeon

Received: 3 October 2024
Revised: 30 October 2024
Accepted: 31 October 2024
Published: 4 November 2024

1. Introduction

In modern cryptography, block ciphers serve as fundamental building blocks to secure data across various applications, including communication protocols, cloud storage, and digital transactions. Block ciphers function by encrypting data in fixed-size blocks, ensuring the confidentiality of information through complex mathematical algorithms [1]. Popular examples of block ciphers include AES (Advanced Encryption Standard) and DES (Data Encryption Standard), both of which have been widely adopted for securing sensitive information. However, the increasing proliferation of resource-constrained devices, such as Internet of Things (IoT) gadgets, smart cards, and embedded systems, has led to the demand for cryptographic algorithms that are secure and lightweight in terms of computational and memory requirements.

1.1. Lightweight Block Ciphers (LWBCs): Necessity and Importance

The explosion of interconnected devices in the IoT era brings unique challenges in ensuring data security. Though highly secure, traditional block ciphers like AES tend to be resource-intensive, requiring significant computational power and memory, which can be impractical for constrained environments. Devices such as RFID tags, wireless sensor networks (WSNs), and embedded systems are characterised by limited energy, processing power, and memory capacity. Therefore, the cryptographic operations required to secure these systems must be optimised to minimise resource consumption without sacrificing security. This is where lightweight block ciphers (LWBCs) become crucial [2].

Lightweight block ciphers are designed to provide security in environments with constrained resources. Their primary goal is to offer robust encryption with minimal

computational overhead, making them well-suited for IoT, smart grids, and mobile devices. Given the surge in cyber threats targeting low-resource devices, the necessity of LWBCs becomes clear. There is an urgent need to secure these systems without exhausting their limited power and processing capabilities [3]. Additionally, with the growing focus on edge computing and smart cities, LWBCs will be critical in securing large-scale real-time data transactions.

1.2. Features of Lightweight Block Ciphers

Lightweight block ciphers differ from their traditional counterparts in several ways, often optimised for efficiency and adaptability to constrained environments. Some of their distinguishing features include the following:

- Smaller block sizes: LWBCs use smaller block sizes (e.g., 64 bits rather than the typical 128 bits of AES) to reduce the memory footprint and computational load.
- Simple key schedules: LWBCs often have simpler key scheduling algorithms, which help minimise the time and resources needed to generate encryption keys.
- Reduced round functions: Fewer encryption rounds are implemented, reducing the number of complex operations while maintaining adequate security.
- Optimised S-box designs: LWBCs use smaller and simpler substitution boxes (S-boxes) to lower the processing demands during substitution steps.

Some well-known lightweight block ciphers include PRESENT, CLEFIA, and Simon/Speck. Each is designed with specific hardware and software optimisations to fit within the constraints of its target environment.

1.3. Pros and Cons of Lightweight Block Ciphers

The use of lightweight block ciphers has advantages and limitations, particularly compared to traditional block ciphers, which is demonstrated in Table 1.

Table 1. Pros and cons of lightweight block ciphers (LWBCs).

Pros	Cons
Low resource consumption: LWBCs are designed to use less power, memory, and processing capacity, making them ideal for devices with limited resources.	Weaker security margin: due to their smaller block sizes and reduced round functions, LWBCs may offer a lower security margin than traditional block ciphers like AES.
High efficiency in constrained environments: they are specifically optimised for performance in devices with constrained energy sources, like IoT devices and smart cards.	Limited to specific use cases: while suitable for low-resource environments, LWBCs may not be as effective in high-security applications requiring large-scale encryption.
Faster encryption and decryption: with fewer rounds and optimised operations, LWBCs often provide faster encryption and decryption processes, enabling real-time data security.	Potential vulnerability to specific attacks: LWBCs' reduced complexity may expose them to cryptanalytic attacks that target their specific design trade-offs.
Adaptable for both hardware and software implementations: LWBCs can be implemented on a wide range of platforms, from tiny microcontrollers to more powerful processors.	Smaller key sizes: LWBCs may employ smaller key sizes, potentially reducing their resilience to brute-force attacks, especially as computational power increases.

As the demand for secure communications in resource-constrained environments grows, the importance of LWBCs becomes undeniable. They offer a pragmatic solution for the encryption needs of IoT networks, RFID tags, and mobile devices. However, their implementation requires a careful consideration of security trade-offs, as lightweight ciphers, while efficient, may not always provide the same level of robustness as traditional cryptographic algorithms.

Despite its potential, significant challenges must be addressed to successfully implement the IoT [4]. These challenges primarily relate to the energy efficiency and security of IoT devices [5]. Researchers have proposed lightweight cryptography as a promising solution to address these issues. This cryptographic approach is designed for IoT applications and balances safety, performance, and energy efficiency. Doing so may facilitate the adoption and expansion of future IoT technologies.

1.4. Background of This Study

Over the past few years, our research team has been engaged in designing a lightweight block cipher (LWBC) [6] and its constituent components, namely the substitution box (S-Box) [7], permutation box (P-Box) [8], and key management field [9]. These components were tested individually to assess their performance. Currently, our research is focused on investigating the proposed LWBC's power consumption by integrating all the components and comparing the proposed Cipher with other lightweight ciphers.

This study aims to evaluate the proposed cipher's energy efficiency under varying operational circumstances. Specifically, we seek to quantify the cipher's power consumption and analyse its performance under different operational scenarios. The results of this investigation will provide valuable insights into the proposed cipher's energy efficiency and potential suitability for practical applications.

The research addresses the crucial trade-off between energy efficiency and security by analysing the power usage of the proposed LWBC for IoT. The primary goals of this research include evaluating energy efficiency, comparative analysis, security power trade-off, and practical application.

Given the inherent energy constraints of IoT devices, it is necessary to measure the power consumption of the proposed cipher in several operational conditions to determine its energy efficiency. To assess its viability, this research compares the cipher's energy efficiency to currently used IoT cryptography techniques. The study also examines the trade-off between power consumption and security strength, which is crucial in IoT contexts with limited resources. The research demonstrates the practical application of the cipher on the IoT and confirms its suitability for the proposed cryptographic solutions.

The proposed cipher employs a 64 bit plaintext block and a 64 bit key from 32 bit pre-distributed partial keys. The encryption procedure involves four steps in each round: XORing with the key, traversing an S-box, applying an additional layer, and ultimately passing through a P-box. The cipher balances complexity and efficiency by minimising the number of encryption rounds. This objective is achieved by incorporating a strong S-box and P-box, which significantly enhance the security of the encryption process.

The study's findings have significantly improved IoT security, particularly for devices with limited battery life. The study introduces a cipher that enhances security across multiple IoT domains, sheds light on the importance of energy-efficient cryptographic design, and contributes to creating safe and energy-efficient algorithms for the future. Additionally, the study highlights the crucial need for designing cryptographic protocols tailored to contexts with limited power. These findings bear significant implications for IoT security and serve as a stepping stone for further research in this domain.

This research contributes to IoT security by comprehensively evaluating the power consumption, use of other resources, and security aspects of the LWBCs we developed [6–9]. The key contributions of this study are as follows:

- It developed a physical setup to measure the energy consumption of security algorithms on Arduinos, targeting IoT resource requirements.
- It introduced a scalable approach to evaluate power consumption across different platform algorithms for IoT devices.
- Created an architecture that allows the flexible analysis of security applications on various systems.
- It utilised the Arduino NodeMCU V3 platform for energy consumption analysis, leveraging its compatibility with IoT security needs.

- It employed the Qoitech Otii Arc to measure energy consumption accurately, utilising the shunt resistor methodology for a systematic analysis. It also offers high sampling rates and accuracy and is suited for low-resource IoT devices.
- It demonstrated the proposed LWBC's energy efficiency, with an average power consumption of 4.5 μJ/bit, making it suitable for resource-constrained IoT devices.

The rest of the paper is organised as follows: it begins by discussing key performance metrics for IoT applications (Section 2) and the challenges of deploying ciphers across diverse IoT environments (Section 3). Section 4 analyses energy efficiency in cryptographic protocols, exploring lightweight cipher designs to balance security and power use. A comparison of existing lightweight block ciphers with the proposed cipher is provided in Section 5, while Section 6 outlines methods for evaluating power usage in these protocols. The proposed lightweight block cipher (LWBC) is detailed in Section 7, followed by the experimental setup for measuring its energy consumption in Section 8. Results and comparisons with other ciphers are discussed in Section 9, leading to the Conclusion (Section 10), highlighting the LWBC's effectiveness and future potential for energy-efficient security in IoT.

2. Performance Metrics in IoT Applications

Performance metrics in IoT applications are critical in assessing functionality, reliability, efficiency, and suitability for different use cases. Below is a detailed breakdown of the key performance metrics, along with implications for various types of IoT applications.

2.1. Latency

- Definition: The time data travels from the IoT device to the central server or endpoint and back.
- Implications:
  - Critical for real-time applications: low latency is crucial for real-time applications like healthcare monitoring (e.g., heart rate or glucose monitoring) and autonomous driving, as high latency could lead to delayed responses and potentially life-threatening situations;
  - Moderately important for industrial IoT (IIoT): manufacturing processes and machine control require low latency to ensure synchronisation and safety but may tolerate slightly higher latency than real-time healthcare;
  - Less critical for smart home applications: smart lighting or thermostat control applications can tolerate higher latency, as responses can take time.

2.2. Reliability

- Definition: The ability of an IoT system to perform consistently over time without failure.
- Implications:
  - High priority for industrial IoT: high reliability is essential in manufacturing and critical infrastructure to avoid costly downtime, production issues, and potential safety hazards.
  - Critical for healthcare applications: reliability is vital to patient safety. A failure in medical monitoring devices could lead to undetected health risks.
  - Moderately important for consumer IoT: a temporary failure may only cause inconvenience for smart home devices. However, reliability remains essential to avoid user frustration and maintain trust.

2.3. Scalability

- Definition: The ability of the IoT system to handle an increasing number of devices and users.
- Implications:

- Essential for smart city applications: as urban IoT infrastructure expands, systems must accommodate more devices like sensors, traffic cameras, and public service monitors without degrading performance;
- Important for large-scale industrial applications: IIoT systems in factories must support scaling to hundreds or thousands of devices as new equipment or processes are added;
- Less critical for small consumer IoT networks: for single households or small setups, scalability is less critical but should still support additional devices as technology evolves.

2.4. Data Throughput

- Definition: The volume of data that the IoT network can handle in a given time period.
- Implications:
  - High requirement for video surveillance and AR/VR applications: applications transmitting high-definition video or augmented reality data, such as smart security cameras, require high throughput to avoid data loss or buffering;
  - Moderate requirement for industrial monitoring: IIoT applications with sensors producing steady streams of data require adequate throughput to handle this flow but do not have the same intensive demands as video applications;
  - Low requirement for basic sensor networks: basic environmental sensors (e.g., temperature, humidity) in agriculture or home settings generate smaller amounts of data and thus require lower throughput.

2.5. Energy Efficiency

- Definition: The power consumption of IoT devices and their ability to function effectively with minimal energy.
- Implications:
  - Critical for remote and battery-powered applications: IoT devices used in agriculture, wildlife tracking, and remote monitoring often rely on battery power, making energy efficiency essential to extend operational life and reduce maintenance;
  - Important for wearable and healthcare devices: in wearables and health monitoring, long battery life improves usability and ensures continuous monitoring;
  - Less important for mains-powered applications: for devices that are consistently plugged in, such as home assistants or industrial IoT equipment, energy efficiency is beneficial but not a primary concern.

2.6. Bandwidth

- Definition: The maximum amount of data that can be transmitted over a network in a specific time frame.
- Implications:
  - Critical for high-data applications: surveillance systems, video streaming, and smart grids require high bandwidth to handle large volumes of data;
  - Moderate need for industrial automation: IIoT systems often generate moderate data flows from numerous sensors, necessitating reliable but not excessive bandwidth;
  - Low requirement for small IoT devices: low-power, small data-transmitting devices (e.g., simple environmental sensors) can operate effectively on lower bandwidth, making them suitable for low-power wide-area networks (LPWANs).

2.7. Security

- Definition: The resilience of IoT systems against unauthorised access, data breaches, and other security threats.
- Implications:

- Essential for healthcare and financial applications: any application handling sensitive health or financial data must have robust security to protect user privacy and meet regulatory compliance;
- Critical for industrial IoT and smart grids: security breaches in IIoT or critical infrastructure can lead to operational disruptions, safety hazards, and even national security risks;
- Important for consumer IoT: while security is often less prioritised in consumer devices, breaches can lead to personal data leaks and network vulnerabilities that impact user trust.

2.8. Interoperability

- Definition: The ability of IoT devices and systems to work seamlessly with other devices, systems, or networks.
- Implications:
  - Highly relevant for smart homes and cities: devices from multiple vendors must interact to ensure a cohesive smart environment, whether for home automation or urban infrastructure;
  - Important for healthcare: health IoT applications need to integrate data across different platforms (e.g., hospitals, wearables) for comprehensive patient care;
  - Moderately important for industrial IoT: while IIoT can benefit from interoperability, many industrial environments use proprietary systems, so compatibility within the facility's systems is prioritised.

2.9. Accuracy and Precision

- Definition: The degree to which the data collected by IoT devices is correct and precise.
- Implications:
  - Crucial for healthcare and environmental monitoring: accuracy is vital to ensure reliable health assessments and environmental data, as incorrect data could lead to misinformed decisions;
  - Important for industrial IoT: accurate data from machinery sensors can prevent breakdowns and optimize performance;
  - Less critical for some consumer applications: while still beneficial, precision is often less critical for applications like smart lighting or thermostats, where minor deviations in data do not significantly impact the outcome.

2.10. Cost Efficiency

- Definition: The overall cost-effectiveness of deploying, maintaining, and operating IoT devices.
- Implications:
  - Essential for large-scale deployments: smart cities and large industries need cost-effective solutions to manage thousands of devices while maintaining service quality;
  - Important for consumer IoT market: cost efficiency determines consumer adoption of smart home devices, as high costs can deter users;
  - Moderately important for specialised applications: cost efficiency is secondary to performance and reliability for critical applications like healthcare or military IoT.

A Summary of Metric Relevance for Different IoT Applications is given in Table 2:

Table 2. A summary of metric relevance for different IoT applications.

Metric	Smart City	Industrial IoT	Healthcare	Consumer IoT	Remote Monitoring
Latency	High	Moderate	High	Low	Moderate
Reliability	High	High	High	Moderate	High
Scalability	High	Moderate	Moderate	Low	High
Data Throughput	High	Moderate	High	Moderate	Low
Energy Efficiency	Moderate	Moderate	High	Moderate	High
Bandwidth	High	Moderate	High	Low	Low
Security	High	High	High	Moderate	High
Interoperability	High	Moderate	High	High	Moderate
Accuracy and Precision	High	High	High	Moderate	High
Cost Efficiency	High	High	Moderate	High	Moderate

Understanding these metrics enables IoT designers and stakeholders to optimize system performance, prioritise security, and address specific requirements across diverse applications, ensuring that IoT solutions fit for purpose.

3. Challenges and Considerations for Cipher Deployment in Diverse IoT Ecosystems

Deploying a cipher in diverse IoT ecosystems involves navigating various challenges and considerations due to the IoT networks' unique characteristics and demands. These networks are heterogeneous, containing devices with varying processing capacities, power limitations, and security requirements, which can complicate the implementation of a uniform encryption standard. The discussion below explores the key challenges and considerations for deploying a cipher in IoT environments with high data throughput requirements, varied device types, and operational constraints.

3.1. Performance Impact on Low-Powered Devices

- Challenge: IoT devices span many capabilities, from high-performance to low-power sensors. Many low-powered devices, particularly those in remote or battery-operated applications, have limited computational resources and may need help with complex encryption algorithms.
- Consideration: To ensure that the cipher performs efficiently across all devices, lightweight encryption protocols, such as those based on symmetric key encryption (e.g., AES), may be preferable. Alternatively, adopting lightweight versions of asymmetric encryption algorithms can balance security needs with computational constraints.

3.2. Latency and Data Throughput

- Challenge: Certain IoT applications, such as video surveillance, autonomous systems, and industrial monitoring, require high data throughput and minimal latency. Applying a cipher with significant processing overhead can introduce delays, impacting the system's real-time performance.
- Consideration: In high-throughput systems, choosing a low-latency cipher is essential to maintaining performance. Stream or block ciphers with smaller block sizes may be suitable in these environments, as they generally offer faster encryption and decryption processes. Optimising the encryption process to handle large volumes of data without disrupting system responsiveness is crucial.

3.3. Heterogeneity of Device Types

- Challenge: IoT ecosystems often contain devices from various manufacturers with diverse architectures, operating systems, and communication protocols. Ensuring compatibility and interoperability between these devices while maintaining a consistent encryption standard can be complex.

- Consideration: Using standardised ciphers recognised across the industry, such as AES or elliptic-curve cryptography (ECC), may improve compatibility. Implementing encryption algorithms at a protocol level, for instance, using TLS or DTLS over networks can provide uniform encryption support across heterogeneous devices without requiring changes to individual device software.

3.4. Energy Efficiency and Battery Life

- Challenge: IoT devices deployed in remote or hard-to-reach locations often rely on battery power. Applying energy-intensive ciphers may significantly reduce battery life, requiring frequent maintenance or replacement and leading to potential operational downtime.
- Consideration: Energy-efficient ciphers, such as those optimised for minimal processing and memory usage, are ideal for battery-powered IoT devices. Implementing encryption algorithms with adaptive power management, which selectively applies full encryption or lightweight alternatives based on current power levels, can extend device lifespans in power-constrained environments.

3.5. Scalability and Key Management

- Challenge: Large-scale IoT ecosystems, such as smart cities or industrial IoT, involve managing encryption keys across thousands or even millions of devices. These challenges ensure secure and efficient key distribution, storage, and renewal.
- Consideration: Adopting centralised key management systems, such as public key infrastructure (PKI), can facilitate secure and scalable key handling. However, in specific IoT scenarios, decentralised or lightweight key management protocols like the Datagram Transport Layer Security (DTLS) protocol can be effective. Incorporating periodic key rotation mechanisms and mutual authentication protocols can enhance security and scalability.

3.6. Security vs. Performance Trade-Off

- Challenge: Balancing strong security with system performance remains a critical concern. High-level encryption protocols add computational load, hindering performance in IoT environments requiring immediate data processing and response, such as autonomous driving or health monitoring systems.
- Consideration: Adaptive encryption protocols can offer flexibility, adjusting security levels based on the device's capabilities and the sensitivity of the transmitted data. For instance, compassionate data can undergo full encryption, while less critical information may use lighter encryption schemes, optimising the performance–security trade-off.

3.7. Compliance with Data Privacy Regulations

- Challenge: Different regions have unique data privacy regulations (e.g., GDPR in Europe, CCPA in California) that impose stringent data protection standards, which may conflict with the technical capabilities of specific IoT devices.
- Consideration: Ensuring the chosen cipher complies with relevant regulations while remaining functional across IoT devices of varying capacities is essential. This may involve using compliant, industry-standard encryption algorithms and adopting privacy-focused measures like data minimisation to limit sensitive data exposure on devices with lower security capabilities.

3.8. Security for Data in Transit and at Rest

- Challenge: IoT systems generate a high volume of data that moves across networks and is stored on various devices. Protecting this data during transmission and when stored is essential to mitigate interception and unauthorised access risks.

- Consideration: Encrypting data in transit with secure protocols like TLS or DTLS is widely adequate for IoT networks. In contrast, data at rest can be protected using hardware-based encryption on devices with insufficient storage and processing power. Devices with limited capabilities may benefit from lightweight encryption at the firmware level to secure data locally without significantly impacting performance.

Successfully deploying a cipher across diverse IoT ecosystems requires a nuanced approach, carefully considering device capabilities, network requirements, and operational constraints. Lightweight, flexible encryption solutions offer an adaptable option, while standardisation and interoperability improve compatibility across heterogeneous systems. Addressing these challenges with adaptable, low-latency, and energy-efficient encryption methods will ensure secure and scalable IoT systems that maintain performance standards across various applications.

4. Evaluating Energy Efficiency for Lightweight Cryptographic Protocols

This section thoroughly analyses the energy consumption of cryptographic algorithms in IoT devices, specifically focusing on finding the right balance between security and energy efficiency. The section also examines the key features of lightweight ciphers and reviews relevant research to understand design enhancements that minimise power usage in IoT settings.

4.1. Features to Consider for Power Consumption Analysis of LWBC

Power consumption analysis for LWBCs has gained considerable attention in resource-constrained environments [10]. Examining the various features associated with LWBCs is crucial to balance security requirements and energy efficiency. In this regard, the following features are worth considering:

Firstly, a comprehensive evaluation of the cipher overhead is essential when implementing a lightweight block cipher (LWBC), as it necessitates an analysis of the additional burdens introduced, such as message expansion and the requirement for extra computational rounds. Message expansion can result in increased encrypted message sizes, leading to greater bandwidth consumption and extended processing times. At the same time, additional computational rounds may exacerbate the processing workload, thus impacting the overall performance and efficiency. Therefore, the meticulous management of these elements is crucial to minimise unnecessary protocol overhead, streamlining processing, and enhancing energy efficiency; this is particularly significant in resource-constrained environments or mobile devices where higher energy consumption can accelerate battery depletion. Striking a balance between robust security measures and reduced overhead is imperative to achieve optimal energy efficiency while maintaining the integrity of the cipher against potential vulnerabilities, a necessity for the effective deployment of cryptographic algorithms across various applications [11].

Secondly, examining how much the LWBC (lightweight workload-based controller) supports features like parallelisation and piping is crucial, as these capabilities significantly enhance computational performance. Parallelisation allows for the simultaneous execution of tasks across multiple cores, leading to a noticeable reduction in execution time and the ability to handle complex computations more efficiently. Meanwhile, piping facilitates the direct flow of data between processes, allowing the output of one task to serve as the input for another, thereby streamlining workflows and minimising resource consumption. By effectively leveraging both parallelisation and piping, the LWBC can maximise the benefits of multicore architectures, resulting in lower energy consumption and improved overall system performance. A thorough investigation of these features is essential to fully understand their impact on efficiency and effectiveness in various computing environments [12].

Thirdly, evaluating memory usage is crucial for optimising the applications' memory requirements, particularly when managing key storage and data structures. By carefully analysing and refining how memory is allocated and utilised, developers can significantly reduce the overall footprint of their applications. This optimisation enhances performance

and minimises power consumption, which is particularly important for devices with limited memory resources, such as mobile phones and embedded systems. By striking a balance between efficiency and functionality, developers can ensure that their applications run smoothly while conserving battery life and maximising the capabilities of the hardware they operate on [13].

Fourthly, the energy-aware cipher design focuses on developing lightweight block ciphers (LWBCs) that prioritise energy efficiency, which is increasingly vital in resource-constrained environments such as mobile devices and IoT systems. By exploring this design approach, researchers can identify ciphers that maintain robust security standards and incorporate mechanisms to dynamically adjust their operations based on the available energy resources and prevailing power conditions. This adaptability can lead to more sustainable cryptographic solutions, allowing devices to conserve energy while performing necessary encryption tasks effectively. As a result, integrating energy-awareness in cipher design could significantly enhance the longevity and performance of battery-dependent systems in various practical applications [14].

Fifthly, to effectively evaluate the efficiency of various lightweight block ciphers (LWBCs), it is essential to employ quantitative metrics that specifically measure and compare power consumption. Key metrics such as energy per encryption and energy per bit serve as concrete benchmarks, allowing for a clearer understanding of the energy demands associated with each cipher during operation. By utilising these metrics, researchers and developers can identify which LWBCs provide robust security and optimise energy use, making them more suitable for deployment in resource-constrained environments like embedded systems and mobile devices. This approach enhances the performance evaluation process but also aids in promoting more energy-efficient cryptographic solutions in the industry [15].

Finally, real-world testing is essential for accurately assessing the power consumption of the LWBC in practical scenarios, as it allows for the direct observation of how the system performs on actual target devices. Considering factors such as communication delays, idle times, and varying workloads, this approach comprehensively explains the device's energy efficiency under realistic conditions. This kind of testing not only highlights the operational challenges faced by the system but also reveals opportunities for optimisation, leading to better energy management strategies and improved performance in real-world applications.

By considering these features in the context of power consumption analysis for an LWBC, informed decisions can be made to achieve the desired balance between security requirements and energy efficiency.

4.2. Related Works

In the literature review for optimising the design to reduce power consumption in IoT end devices, several studies have been examined.

High Throughput Architectures for Lightweight

Crypto-primitives: A study by Mishra et al. delves into high-throughput architectures for substitution modules in lightweight cryptographic primitives, emphasising their suitability for pervasive computing. The research focuses on hardware implementation to enhance speed while optimising the physical area and power consumption. The resulting architectures demonstrate high throughput and reduced energy consumption, making them well-suited for IoT environments [16].

Cryptographic security of the ANU-II block cipher: Fan et al. critically evaluate the cryptographic security of the ANU-II ultra-lightweight block cipher, which is designed for IoT devices. The cipher is noted for its minimal hardware resource requirements, low power consumption, and rapid encryption capabilities. However, the research identifies and addresses specific security vulnerabilities in ANU-II, particularly in its resistance to differential cryptanalysis, and proposes an improved cipher version [17].

Serial hardware architectures for the Piccolo algorithm: Mhaouch et al. propose six serial hardware architectures for the Piccolo lightweight algorithm, which uses a 128 bit key

length. These architectures are assessed based on hardware resource usage, latency, and throughput criteria. Security evaluations of these architectures demonstrate the robustness of the Piccolo block cipher against statistical attacks, affirming its appropriateness for lightweight applications that prioritise privacy [18].

This study analyses the energy consumption of 3G, GSM, and WiFi networks, highlighting the high tail energy overhead in 3G and GSM. It proposes TailEnder, a protocol that optimises energy usage by scheduling data transfers for delay-tolerant apps and prefetching data for others like web search. Evaluations show that TailEnder reduces energy consumption and improves performance, enabling 60% more news updates and 50% more web queries compared to default policies [19].

Another research proposes Secure and Energy Efficient Prefetching (SEEP) to enhance security and reduce energy consumption in smartphone prefetching systems. SEEP uses a local proxy for data validation and a remote proxy for encrypted storage, operating transparently within the existing browser–server framework. It ensures confidentiality, resists replay attacks, and reduces energy usage by one-fourth and data transmission by 95% compared to traditional prefetching over Wi-Fi [20].

Ming et al. [21] introduce a service-specific end-to-end energy-efficiency model to analyse energy consumption across different applications, from messaging to virtual reality. It shows that smartphones consume the most energy for web browsing and messaging, while LTE networks dominate for data-heavy applications like video streaming and VR. The study suggests that using small cell offloading and mobile edge caching can reduce energy consumption by over four-fifths.

These studies contribute to understanding design optimisation in LWBCs, focusing on enhancing power efficiency for IoT devices while maintaining high security and performance standards.

Common implementation [22]: This study examined the runtime performance of encryption techniques. The absence of other measurements reflects a focused investigation of how long the encryption process takes without considering system stress, throughput, or power usage.

Soft profiling [23,24]: These studies did not assess the specified performance indicators. This suggests that the analysis of encryption algorithms may focus on theoretical or qualitative aspects rather than quantitative ones. The UPS Battery [23] is thoroughly assessed in these tests, comprehensively evaluating four key metrics: runtime, workload, throughput, and power consumption. Using a UPS battery as a methodology suggests a potential emphasis on the performance of encryption algorithms when power is limited or reliant on portable batteries.

External measurement [25]: These studies evaluated runtime, throughput, and power consumption but did not examine workload. This method emphasises the importance of efficiency and energy considerations in encryption algorithms, namely their speed and power consumption, which is critical for IoT devices.

In the next section, we briefly describe some examples of LWBCs that were designed considering the abovementioned discussions.

5. Comparison of Lightweight Block Ciphers with the Proposed Block Cipher

This section discusses several LWBCs compared with our proposed cipher [6]. Each block cipher's main characteristics are described, highlighting their distinct characteristics and efficiency in ensuring secure communication in IoT devices with limited resources.

RECTANGLE (a bit-slice lightweight block cipher) [26]: This compact substitution permutation network (SPN) cipher operates on 64 bit blocks and uses 80 and 128 bit keys. It performs its encryption or decryption process through 24–32 cycles. The system includes 16 parallel 4×4 S-boxes and three rotational permutations. Building upon the cryptanalysis of PRESENT, this innovation incorporates a unique S-box and an asymmetrical permutation layer. RECTANGLE is proficient in both hardware, with a capacity of 1467 GE for 80 bit keys and a speed of 246 Kbps, and software, with a performance of 5.38 cycles per byte on

Intel SSE. This cryptographic algorithm is energy efficient and suitable for lightweight and rapid implementations.

PRESENT (an ultra-lightweight block cipher) [27]: The PRESENT cipher, which meets lightweight conditions, significantly advances LWBCs. It has been standardised in ISO/IEC 29192 [28]. The encryption algorithm utilises 80 and 128 bit keys, operates on 64 bit blocks, and employs 31 rounds. It is built upon an SPN structure and incorporates a distinctive single S-box architecture to optimise hardware efficiency. The 80 bit version of the algorithm necessitates 1030 GE for its execution. Software solutions exhibit a condensed code size and perform excellently on microcontrollers. Nevertheless, it is susceptible to side-channel, related-key, biclique, and differential attacks, particularly on variants with fewer rounds.

Piccolo (an Italian word that means small or little) [18,29]: This block cipher uses a generalised Feistel network to process blocks of 64 bits with either 80 or 128 keys. The device is highly energy-efficient, particularly the 80 bit key version, which has a tiny size of 432 GE. An additional 60 gate area (60 GE) is needed for decryption. Piccolo uses multiplexers and scan flip-flops to store data states and utilises AND-NOR and OR-NAND gates for performing operations, eliminating the need for extensive key storage. The software utilises 2434 bytes of code and 79 bytes of RAM. Nevertheless, it exhibits a low throughput of 7.8 Kbps. The security of Full-roundPiccolo-80 has been assessed by biclique cryptanalysis, revealing that Piccolo-128 offers a somewhat higher level of security.

PRINT (based on integrated circuit printing) [30]: This cipher employs 48 and 96 rounds, with 80 and 160 bit keys, and 48 and 96 bit blocks. The process of IC printing, specifically PRINTcipher-48 and 402 GE, as well as EPC encryption, specifically PRINTcipher-96 and 726 GE, involves the use of 3 bit operations. The software implementation is wasteful because it unconventionally utilises bits. PRINT cipher is currently investigating this application domain but must be prepared for implementation. Although it is impossible to execute related-key attacks on IC printing, they have been successfully demonstrated on the full-round cipher.

ICEBERG (metaphorically reflect to an iceberg) [31,32]: This cipher is a fast and complex encryption algorithm that employs 128 bit keys and 64 bit blocks in 16 rounds. Reconfigurable hardware enables the modification of critical parameters in every clock cycle without any decrease in performance and allows for generating round keys in real-time. It efficiently performs encryption and decryption using 5800 gates at 400 Kbps. The most renowned attack is differential cryptanalysis performed on eight rounds. Modern ciphers employ this structure to achieve efficient encryption and decoding at a low cost.

HIGHT (high-security and lightweight) [33]: HIGH is a cipher that uses 128 bit keys and 64 bit blocks throughout 32 rounds. It circumvents the use of S-boxes by relying solely on fundamental computations. The minimum hardware version requires a 2608 GE for a data transfer rate of 188 Kbps. The cryptographic algorithm has seen multiple attacks, such as impossible differential, related-key, biclique, and zero-correlation attacks, on both 26 and 27 round variants.

TEA (tiny encryption algorithm) [34]: TEA is a lightweight block cipher designed to offer simplicity and efficiency with minimal computational resources. It operates on 64 bit data blocks using a 128 bit key, and its structure involves 64 Feistel rounds to ensure security through the repeated mixing of data and key material. The algorithm's design emphasizes ease of implementation, with a minimal code footprint suitable for embedded systems and constrained environments. However, TEA is vulnerable to key-related attacks, such as equivalent keys and weak key schedules, prompting the development of revised versions like XTEA and XXTEA to address these vulnerabilities.

6. LWBC Power-Usage Evaluation Techniques

The assessment of encryption method performance, especially in battery-limited portable wireless devices, heavily relies on power consumption. Assessing the energy usage of a low-weight block cipher requires a comprehensive methodology. This article examines three separate measurement categories: software profiling for rapid comparisons,

battery evaluation for insights into real-world usage, and external assessment for the in-depth analysis of individual components. Every method has distinct benefits that cater to specific research objectives and limitations in the available resources. An in-depth analysis of all three aspects thoroughly comprehends the algorithm's performance characteristics, which is essential for optimising and implementing it in instances with limited resources.

6.1. Software Profiling

Software profiling uses software models to evaluate the power consumption of an encryption technique without the need for hardware intervention. It provides rapid estimations, though the level of accuracy is dependent upon the quality of the model. The categorisation of software profiling techniques for analysing power consumption in lightweight block ciphers can be divided into four primary types: application-level profiling (such as PowerScope), architectural-level modelling (such as Wattch and SimplePower), microprocessor-specific estimation (such as JouleTrack), and simulation-based profiling (such as SimpleScalar). Each method involves a compromise between accuracy, suitability, and the amount of information provided, influencing the choice depending on the specific needs of the power consumption analysis.

PowerScope, developed by Flinn and Satyanarayanan [35], is a specialised tool for profiling app power usage. It connects software behaviour to energy consumption. It combines hardware measurements and software monitoring distinctively to conduct a comprehensive analysis. PowerScope v1.0 is a rapid and software-driven technique for evaluating the power usage of an application. However, it may only partially encompass the entire situation due to its indirect methodology. The overall power usage was determined by integrating the product of the instantaneous current and voltage across time. The power consumption value was estimated by concurrently sampling the current I_t and voltage V_t at a regular time interval Δt. The effective power across n samples was determined by substituting the observed voltage value V_{means} for V_t. The calculation is displayed in Equation (1) [36].

$$E \simeq V_{means} \sum I_t \delta_t \tag{1}$$

Ye et al. [37] presented 'SimplePower', virsion 1.0 a power calculation tool at the register-transfer level that accurately models execution and cycle timing. The software tool 'SimplePower' can simulate executables, allowing for precise power consumption estimations and switch capacitance statistics. It covers many components such as the processor datapath, memory, and on-chip bus. The tool determines the aggregate power consumption of a module by adding up the power consumed at each bit transition. The 'Wattch' and 'SimplePower' models allow computer architects and designers to incorporate power consumption considerations into the initial design phases. Nevertheless, errors in determining the activity factor can result in discrepancies in the predicted power usage.

Brooks et al. [38] developed 'Wattch,' a power modelling program that utilises cycle-level analysis. This model is included in an architectural simulator to estimate the power consumption of CPUs precisely. Their technique primarily focuses on dynamic power consumption p_d, as outlined in Formula (2). The model employs parameters such as v_{dd} and f display, denoting the supply voltage and clock frequency. The parameters in question remain consistent for a specific CPU process technology. The model estimates the load capacitance C, which is determined by the size of the circuit or transistor.

Furthermore, the model incorporates an activity component that varies between zero and one, representing the typical frequency of switching activity initiated by ticks. The activity factor is determined using benchmarks with an architectural simulator or by making assumptions. According to Mishra et al. [39], 'Wattch' provides a swifter, more precise alternative to the currently available power measurement instruments.

$$Pd = CV_{dd}^2 af \tag{2}$$

Sinha and Chandrakasan [40] created 'JouleTrack v0.1', a power estimating software program that does not necessitate specific command characteristics. Their findings revealed a negligible disparity in current consumption among various instructions and even complete programs. It was inferred that the current usage is mainly influenced by the operating frequency and supply voltage rather than the executed program. Nevertheless, the utility of 'JouleTrack' is restricted to quantifying the energy usage of microprocessors. The power consumption of a subroutine executed on a microprocessor can be expressed on a macroscopic level as follows. The variable P_{tot} represents the combined power of both the static and dynamic components. C_L represents the average capacitance switched by the program executed every clock cycle, and f represents the operating frequency [41].

$$P_{tot} = P_{dyn} + P_{stat} = C_L V_{dd}^2 f + V_{ddI} I_{eak} \quad (3)$$

SimpleScalar v3.0e, as highlighted by Naik and Wei [42], is a software tool designed for architectural modelling and simulation focusing on power conservation in software implementation. It facilitates execution-driven simulation, which is more efficient than traditional trace-based methodologies. Nevertheless, it is only guaranteed to consistently offer accurate simulations down to the clock cycle for some architectural types, as there are observed differences between the simulated power consumption and the accurate measurements. This implies that the precision of the system can vary, so it is essential to carefully evaluate its use in situations where power consumption is a concern.

6.2. Battery Evaluation

Battery evaluation is a practical approach to measuring the power consumption of encryption algorithms in IoT devices. It is advantageous due to its simplicity and real-world applicability, eliminating the need for complicated equipment. Under the assumption of steady power consumption, this methodology calculates energy consumption by comparing the decrease in battery capacity between periods of device inactivity and algorithm execution. It directly explains the compromises between security and power effectiveness [43,44]. Nevertheless, the method's dependence on regular usage fails to consider the devices' varying workloads and power states. This could lead to distorted outcomes due to background processes and the absence of accounting for battery degradation and nonlinear discharge characteristics [45,46]. Although there are limitations, battery evaluation is essential for developers prioritising energy saving in battery-operated IoT devices. However, further study is necessary to enhance its accuracy and reliability.

6.3. External Evaluation

The third category comprises techniques that use instruments and electronic equipment to establish a specialised measurement system. This approach is divided into two primary methodologies: external evaluation and onboard evaluation.

Researchers utilised mobile devices, specifically the NOKIA N70, as reference platforms to assess software power usage [47]. This entails altering the power contact of the device to generate two cables, which are subsequently utilised to gauge the current extracted from the battery. This measurement can be conducted using a basic multimeter or a sophisticated oscilloscope. Alternatively, a battery emulator can serve as a substitute for the physical battery. The emulator supplies the phone with electricity and offers precise power consumption measurements. The electrical power (E) is determined by the product of the voltage (v), time (t), and current (I). An inherent benefit of this approach is the consistent and unwavering voltage provided for the whole test duration.

Nevertheless, it cannot accurately assess the energy usage of integrated elements such as the CPU or memory. Creus and Kuulusa [48] presented NOKIA S60 v5.0 software profiling tools that allow developers to determine power usage on the device itself without the need for any external equipment. The analysis can be performed on a mobile device or a personal computer. Nevertheless, this approach must be optimally suited to assessing the power consumption of encryption algorithms. Efforts to apply a cipher on a mobile

device using this approach frequently led to interference with other applications or the device itself.

Creighton et al. [25] conducted a study to quantify the energy usage of apps on devices with restricted resources, specifically focusing on the HP iPAQ 4150. Their configuration entailed sequentially connecting the device between a benchtop power supply and an Agilent 3458A 8½ digit multimeter developed by Keysight Technologies, Inc., based in the USA. The multimeter was assigned to measure the voltage across a resistor at a frequency of 10,000 Hz. The power value was determined by multiplying the resultant voltage with the input voltage and dividing by the resistance, as specified in formula (4) [26]. The energy consumption for each encryption and decryption task was calculated using formula (5) [25], which denotes the frequency of measurements and indicates the execution duration of the encryption algorithm.

$$P_{(t)} = V_{(t)} * (V_{input}/R) \tag{4}$$

$$E_{task} = \Sigma[P_{(t_i)} - P_{idle}] * T \tag{5}$$

On the other hand, Bob and his colleagues at Intel improved the measurement of power utilisation in applications using a precise methodology incorporating data collection (DAQ) technology [49]. This system, which combines a main PC, NetDAQ manufactured by Fluke Corporation based in the USA, and a target PC with motherboards outfitted with sensors, enables thorough power consumption analysis. The researchers achieved precise current and voltage monitoring by attaching the NetDAQ to target components using sensing resistors and wiring it to the host PC. The implementation, backed by logger software on a host PC running an IA32 system, greatly enhanced the precision of power evaluation. It provides a robust framework for analysing the energy use of applications.

This study employs a hybrid methodology to comprehensively assess the proposed LWBC for IoT devices. This approach utilises the accuracy of external measurements using the Otii Arc device and combines it with the practicality of battery evaluation. It examines energy consumption, efficiency factors (such as gate area, throughput, and memory effect), and security in real-world scenarios. This technique effectively combines rigorous technical examination with practical applicability, resulting in a thorough comprehension of the appropriateness of LWBC for energy-efficient encryption in resource-limited contexts.

7. Description of the Proposed Lightweight Block Cipher

Figure 1 illustrates the general architecture of the LWBC method in an SP network. In this diagram, "R" represents a round, and "Rn" indicates the total number of rounds starting with R1 as the initial round, R2 as the second round, and so on. The picture also emphasises the key schedule, noting that each round requires a distinct key. In the context of LWBCs, a "round" refers to a series of operations that are iteratively performed on plaintext to increase security and complexity, making decryption and analysis more difficult. These processes usually entail a blend of permutations, substitutions, and other mathematical functions.

We proposed a simplified block cipher specifically developed to enhance communication security in IoT devices with limited resources. Figure 2 depicts the structure of our proposed encryption algorithm. This cipher achieved higher efficiency and complexity with fewer encryption cycles. The system accepts 64 bits of plain text and utilises a 64 bit key generated from a pool of 32 bit keys. The cipher's functioning in a single round involves four stages: First, the plaintext is XORed with the generated key. Then, the result of this initial step is passed through the suggested Substitution layer, followed by a padding layer, and finally goes through the Permutation layer. The Permutation box (P-box) executes a linear bitwise permutation, whereas the Substitution box (S-box) offers a fixed nonlinear substitution layer.

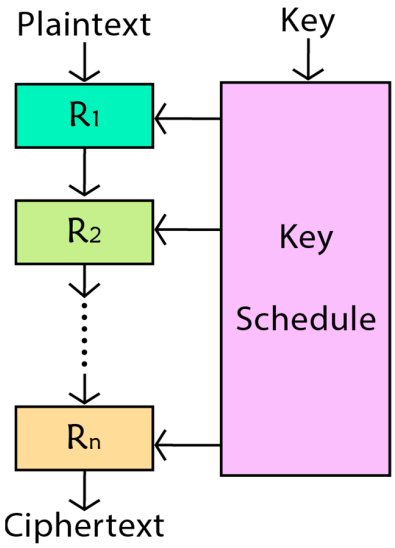

Figure 1. The lightweight block cipher (LWBC) architecture illustrates the iterative process of the round function, key mixing, and nonlinear transformations used in each encryption round. The figure highlights how these components interact to balance security and efficiency, showcasing the steps involved in the encryption process to enhance resistance to cryptanalytic attacks while maintaining low resource consumption suitable for IoT applications.

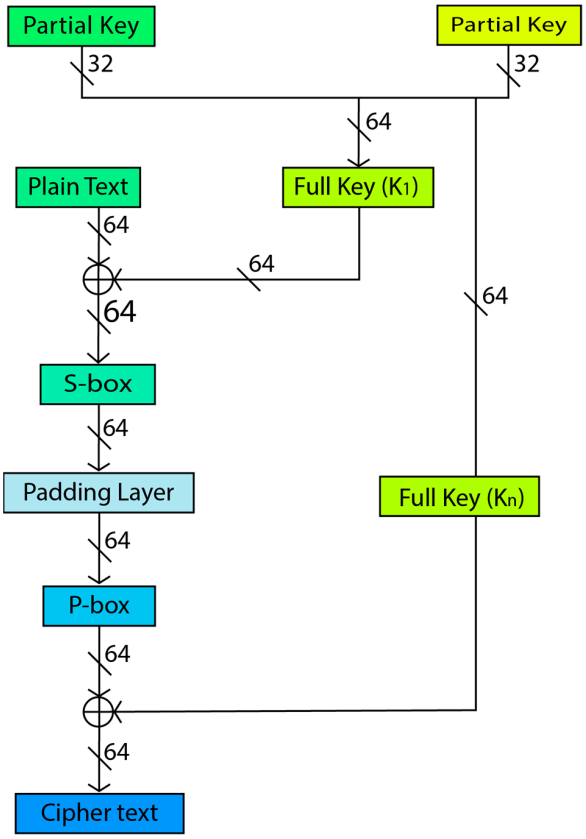

Figure 2. A visual representation of the lightweight block cipher (LWBC) encryption process showcasing the sequence of iterative rounds and the application of nonlinear operations through S-boxes and P-boxes. The figure also illustrates the key schedule mechanism, demonstrating how keys are dynamically integrated in each round to enhance security. This structure underscores the LWBC's balance between computational efficiency and cryptographic strength, optimising it for secure, resource-limited environments such as IoT devices.

7.1. Key Management

Utilising a fixed P-Box involves inherent vulnerabilities, especially in the event of a hacked node. To address this issue, performing an XOR operation between the plaintext and a key is crucial. The plaintext is merged with the key before being input into the S-box and P-box at each stage.

Nevertheless, handling a wide range of keys presents difficulties, necessitating extra storage and processing resources to produce keys that can change over time. We suggest incorporating partial keys pre-loaded onto IoT devices during the initial setup process. This approach is commonly referred to as pre-distribution. This key management strategy primarily emphasises two aspects: the prior distribution of these fragmented keys to minimise resource consumption and the effective use of these partial keys instead of full keys to uphold security integrity.

A detailed explanation of key management algorithms can be found in [9]. The significant parts are highlighted with simple examples to aid understanding.

When deploying IoT devices, a set of partial keys is distributed and embedded into each device before deployment, forming a key pool. This pre-distribution is considered secure since the IoT system is generally safe during this initial phase. Moreover, it is a security mechanism to identify unauthorised users utilising unapproved keys. To minimize storage requirements and safeguard against attackers gaining access to whole encryption/decryption keys in case of a compromised node, each IoT node stores a portion of these keys. Nodes create their unique keys by merging their partial keys using a simple concatenation method to communicate. Using these randomly given partial keys from the pool, nodes can generate several secure keys for different interactions.

This feature of our cipher enhances both the security and data freshness. Consider two devices, A and B, each with a partial key list, such as a, b, c, d, e, and p, q, r, s, t. They agree on a key order choice before encrypting the data. An order list 3, 2, 0, 1, 4 is sent from A to B, and B sends an order list 0, 2, 4, 1, 3 to A. Finally, they use the concatenation function and generate the full key sequence dp, cr, at, bq, es. This dynamic key shuffling and agreement process prevents attackers with only one partial key list from protecting confidential data, even in resource-constrained environments. Regularly refreshing the key order further strengthens the security and ensures data freshness.

7.2. Substitution Box (S-Box)

The S-box and P-box are crucial components in constructing a robust block cipher as they ensure the properties of confusion and diffusion, respectively. The S-box conceals the connection between the ciphertext, key, and plaintext, enhancing the cipher's security. Conversely, the P-box is crucial in obscuring the relationship between the ciphertext and plaintext.

A robust S-box is essential for ensuring the dependability and effectiveness of the block cipher [50]. A 4 bit S-box is advantageous because of its reduced physical space and memory requirements compared to an 8 bit S-box, necessitating a larger gate area and memory usage. We designed an S-box specifically designed for IoT devices with limited resources. The S-box employs a 4×4-bit design well-suited for LWBC. The S-box is generated using an irreducible polynomial derived from the Galois Field. The utilisation of multiplicative inverse and affine translation further enhances the robustness of the S-box. Empirical research has verified that the suggested S-box demonstrates resilience against statistical and differential cryptanalysis [7].

7.3. Padding Layer Between S and P Layers

Our lightweight cipher incorporates an additional padding layer between the S-box and P-box in the SPN structure (Figure 3). This strategic addition aims to achieve a dual benefit: to strengthen security by increasing confusion and diffusion and to improve efficiency by reducing the number of encryption rounds by introducing extra complexity.

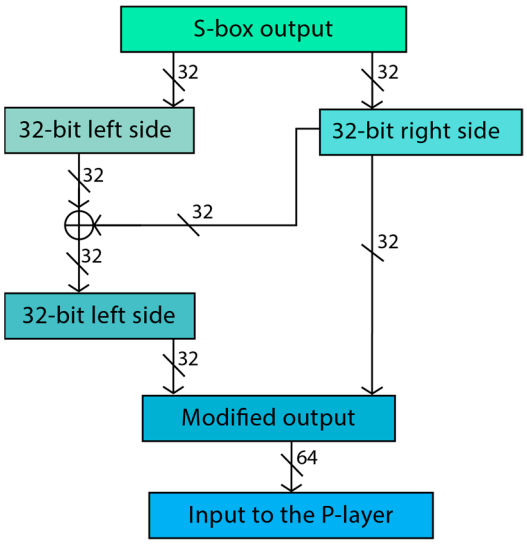

Figure 3. The middle layer of the proposed lightweight block cipher (LWBC), depicting the process of nonlinear transformation through S-boxes and P-boxes, alongside key mixing operations. This layer emphasises the role of nonlinear functions to enhance security by introducing high levels of confusion and diffusion, effectively obfuscating the relationship between the plaintext and ciphertext. The key mixing operations ensure a dynamic key application across rounds, adding an extra layer of complexity to resist cryptanalytic attacks, making the LWBC robust and efficient for IoT applications.

The function of this layer is to split the output of the S-box into two segments, each consisting of 32 bits. It then performs an XOR operation to generate a new segment for the left side and combines it with the right segment. The result is a 64 bit output that resembles an enhanced version of the S-box output. The enhanced data are subsequently transmitted to the P-layer. Our SPN-based cipher offers security comparable to that of the PRESENT cipher while providing faster and perhaps more resilient encryption. By applying a robust S-box to intensify confusion, we decrease the number of rounds by employing a distinctive padding layer, optimising speed and resource efficiency. This design emphasises the importance of a lightweight implementation while ensuring robust security measures against potential attackers.

7.4. Permutation Box (P-Box)

We developed a customised 64 bit P-box for IoT devices with limited resources. This P-box utilises a nonlinear feedback shift register (NFSR) to rearrange bits and improve security. Table 3 is an example of the 64 bit P-box generated by the NFSR. The selection of this 64 bit design method is aimed at reducing the effects on both hardware and software, making it especially well-suited to environments with restricted resources. The cyclic behaviour and feedback mechanism of the NFSR enables effective bit reordering, resulting in robust diffusion and rendering it challenging for attackers to establish connections between input and output bits. The P-box, based on the NFSR, improves the security and efficiency of the cipher by creating unique sequences and eliminating pre-periods. This makes it a viable solution for boosting communication security between IoT end devices.

Figure 4 shows the implementation of the proposed LWBC encryption and decryption mechanism, S-box, and P-box. This process involves generating random keys, converting plaintext into binary format, encrypting the data using substitution and permutation techniques, such as S-box and P-box, and decrypting the cipher text to retrieve the original plaintext.

Table 3. Proposed LWBCs P-box.

i	P(i)	i	P(i)	i	P(i)	i	P(i)
0	51	16	14	32	8	48	34
1	42	17	58	33	56	49	54
2	28	18	3	34	59	50	1
3	16	19	41	35	18	51	43
4	33	20	53	36	39	52	21
5	0	21	37	37	2	53	7
6	13	22	4	38	6	54	63
7	19	23	9	39	11	55	61
8	5	24	26	40	17	56	29
9	38	25	31	41	55	57	22
10	45	26	57	42	35	58	46
11	49	27	20	43	15	59	25
12	44	28	23	44	24	60	52
13	30	29	12	45	40	61	47
14	27	30	60	46	36	62	10
15	48	31	50	47	32	63	62

```
Functions (Proposed lightweight block cipher):
   1. generate_64_bit_keys ():
         o  Generates a list of 64-bit keys by repeatedly combining two 32-
            bit keys.
   2. convert_text_to_binary(text):
         o  Converts plain text into its binary representation (concatenated
            binary values of each character).
   3. encrypt_text (plain_text, keys):
         o  Encrypts plain text using a series of operations (S-box, mid-
            layer, P-box, XOR with keys) in a loop.
   4. decrypt_text (cipher_text, keys, last_encryption_key):
         o  Decrypts cipher text using the reverse encryption operations in a
            loop, starting with the last encryption key.

 Functions (Substitution box):
   1. irreducible_polynomial_selection ():
         o  generates a comprehensive list of all potential polynomials
            within the Galois Field GF (2⁴) to establish operations for
            calculations.
         o  selects an irreducible polynomial from the above list.
         o  generates multiplicative inverse table from the selected
            irreducible polynomials.
   2. generates_Multiplicative_inverse(table):
         o  converts plain text into its binary representation (concatenated
            binary values of each character).
   3. construction_of_S-box(table):
         o  uses  an  algebraic  function  referred  to  as  an  "affine
            transformation" on the hexadecimal table to blend and obscure
            values, resulting in the creation of a robust and secure S-box.

 Functions (Permutation box):
   1. initialises_NFSR ():
         o  initialises NFSR with a preferred 'SEED_SIZE' and
            'feedback_taps.'
   2. Initialises_array_bits (table):
         o  to tracks of which numbers generated by the NFSR.
   3. Generates_array_bits (table):
         o  stores the numbers in 'array' and marks it as seen in 'bits.'
   4. Construction_of_P-box(table):
         o  After the loop it generates all unique numbers in 'array'.
```

Figure 4. Pseudocode algorithm for encryption and decryption in the proposed LWBC.

8. Experimental Setup to Evaluate the Energy Consumption of the LWBC

In this section, we introduce a carefully designed physical structure that measures the energy consumption of security algorithms on Arduinos. Arduinos are a popular choice for IoT development, and our system explicitly targets the resource requirements of security algorithms on these devices. This approach lays the foundation for a scalable method to evaluate different platform algorithms. By highlighting the power consumption of security processes on Arduino, we demonstrate our architecture's versatility and possible

applicability in various scenarios. Our specialised study setup is flexible and enables us to analyse the execution of different security applications on multiple systems.

Explanation for scientific publication:

The above pseudocode provides a comprehensive overview of the encryption and decryption operations in the proposed LWBC. The algorithm comprises several interlinked components:

Key management: the function generate_64_bit_keys() generates dynamic keys by combining 32 bit subkeys, enhancing security through key variability.

Text conversion and encryption: plaintext is converted into binary form, encrypted through iterative rounds using S-box substitutions, P-box permutations, and XOR operations with keys.

S-box construction: the S-box, a critical component for ensuring nonlinearity, is built using irreducible polynomials in $GF(2^4)$ and an affine transformation. This combination ensures that the cipher resists linear cryptanalysis.

P-box construction: the P-box is constructed using an NFSR-based approach to generate unique permutations. This ensures high diffusion, further obfuscating the relationship between input and output data.

Decryption: decryption reverses the encryption operations using the final encryption key as the starting point, ensuring the correct retrieval of the original plaintext.

This modular design ensures the proposed LWBC is both efficient and secure, balancing the requirements of lightweight cryptography with the need for robust resistance against cryptanalytic attacks.

The Arduino NodeMCU V3 is the selected platform for analysing the energy usage of the LWBC algorithm, as shown in Figure 5 [51]. This widely used development board is equipped with a high-performance Tensilica Xtensa® 32-bit RISC processor running at 80 MHz, which offers sufficient processing capability for executing algorithms. Equipped with four megabytes of flash memory and 64 kilobytes of SRAM, it effortlessly stores program code and operational data. The NodeMCU V3 enhances its functionalities by integrating EEPROM, which allows for the secure and durable recording of important LWBC parameters. In addition, the device has Wi-Fi capabilities that follow the 802.11 b/g/n standards. It also has WPA/WPA2 encryption to secure contact with external services. The platform's adaptability is augmented by its 30 digital I/O ports and one analogue input, enabling seamless connection with a wide range of sensors and actuators for LWBC analysis [52].

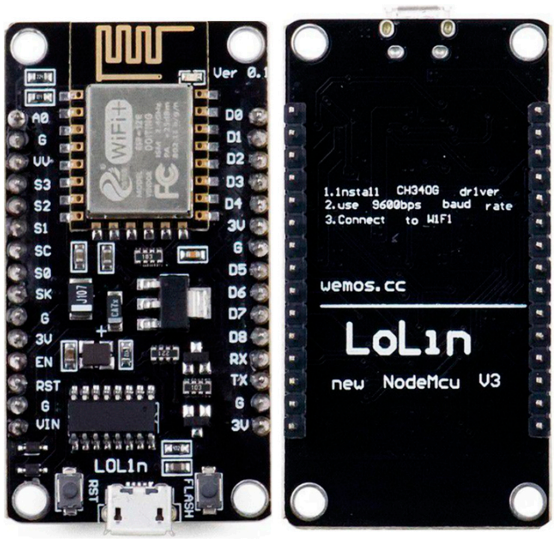

Figure 5. Arduino ESP8266 NodeMCU V3 device front and back view. The NodeMCU V3 development board is an open-source hardware platform based on the ESP8266 Wi-Fi SoC developed by Espressif Systems, headquartered in Shanghai, China.

Our methodology involves measuring the outside of the component, ensuring that our approach remains independent of the device's individual properties. This architectural style's inherent lightweight nature allows for versatile measurement capabilities across various contexts, unrestricted by the need for controlled surroundings.

Determining electrical power entails computing the multiplication of the current (I) passing through the component and its operational voltage (V_{cc}). The voltage is measured directly using a voltage sensor. IoT determines the present electrical flow; we determine by computing the voltage (V_{shunt}) measured across a shunt resistor that is incorporated into the USB power line. The procedure is depicted comprehensively in Equation (6).

$$P = V_{cc} * I = (V_{cc} \cdot V_{shunt})/R \tag{6}$$

The determination of the current flow is derived from Ohm's law, expressed as $I = (V_{shunt}/R)$. The variable represents the resistance of the shunt resistor in this equation. Choosing an adequately low resistance value is essential to minimise the voltage drop at the device's input while guaranteeing that our sensor can detect the drop. In our measurements, we employed the minimum resistance value that our sensor can precisely detect, opting for a shunt resistor with a resistance of 0.02 Ω and ADC measurement point.

To calculate the power consumption of the device (P), we utilise the Formula (6):

This equation enables the computation of power by utilising the device's operational voltage (V_{cc}), the measured voltage across the shunt (V_{shunt}), and the resistance of the shunt resistor (R).

To precisely assess the energy consumption of our LWBC algorithm, we employed the Qoitech Otii Arc, a specialised instrument designed to optimise the energy usage of devices, software, and algorithms. It is beneficial for understanding and improving the energy characteristics of battery-powered devices with low resources, like IoT devices. The Qoitech Otii Arc is a precise and flexible power analyser for IoT applications, especially those involving low-current, battery-operated devices. This device works very well as a flexible source measure unit (SMU) and can measure power in many fields with great accuracy and good detail. The device's high sampling rate of kilo samples per second (kbps) and wide analogue bandwidth of kilohertz (kHz) allow the precise monitoring of fast current fluctuations, making it well-suited for high-frequency situations. The Otii Arc is equipped with user-friendly software compatible with multiple operating systems. It allows for real-time monitoring, data synchronisation, and a simple setup, enabling a thorough study of power usage in IoT devices with no effort [53].

The Otii Arc utilises the shunt resistor technique to achieve precise current measurement in IoT devices. This is a critical process for analysing power consumption trends and enhancing device effectiveness, as Figure 6 depicts. The unit of measurement for power is milliwatts (mW), and the energy efficiency of IoT electrical systems is assessed by analysing their energy consumption. The energy consumption (E) is calculated in joules (J) by multiplying the power (P) in watts (W) by the time (t) in seconds (s), according to the following equation.

$$E = P * t \tag{7}$$

The experimental structure utilises the Otii Arc (Figure 7) as a power source and battery emulation for the Arduino NodeMCU V3 while simultaneously running the LWBC security algorithm. As illustrated in Figure 8, the Arduino's "3V" and "G" terminals are directly linked to the corresponding outputs of the Otii Arc to ensure precise voltage and current measurements. Facilitating data interchange is achieved through a physical connection between the Arduino's UART TX pin and the Otii Arc's UART RX pin. This connection allows for the real-time monitoring and synchronisation of power usage with algorithm execution. The Otii Arc can be linked to a specialised high-capacity USB charging connector to provide an ample power supply for intensive tasks. The Otii software automatically initiates the powering and data recording processes. This process entails the straightforward steps of activating the power supply, adjusting the settings, and pressing the start button.

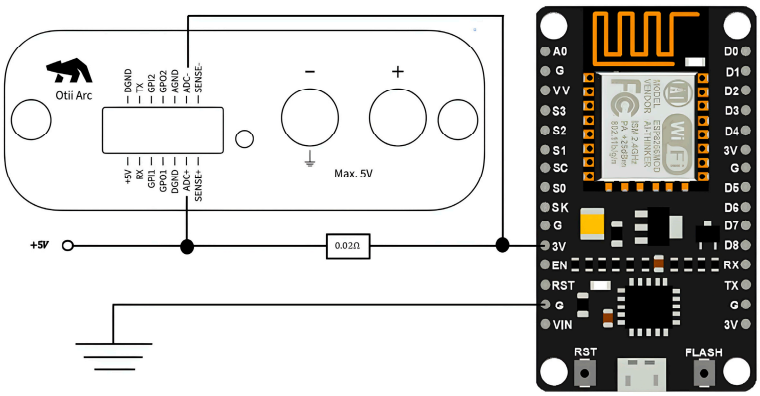

Figure 6. Schematic diagram of a USB power line featuring a shunt resistor and an ADC.

Figure 7. Qoitech Otii Arc power measuring device manufactured by Qoitech AB, a company based in Malmö, Sweden.

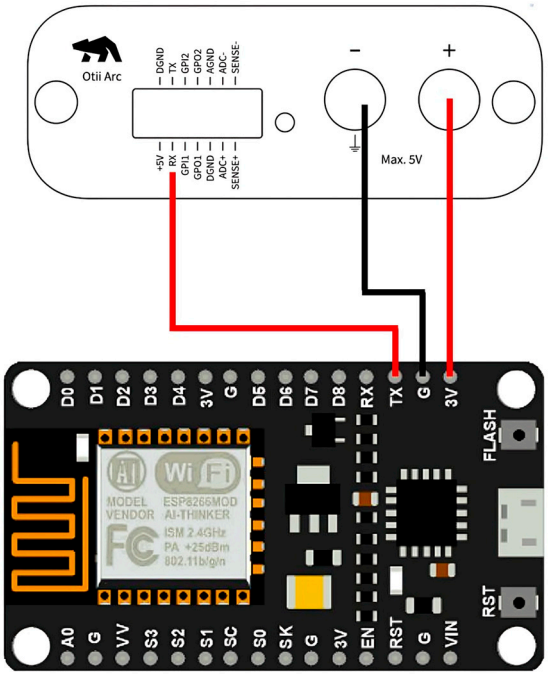

Figure 8. Connection diagram between Otii and IoT device.

The existing methodology meticulously assesses the energy consumption of IoT security algorithms. By employing the ESP8266 NodeMCU V3 in conjunction with the Otii Arc,

we have established the foundation for examining and improving energy efficiency in IoT devices. The upcoming section will explore the findings and consequences of this analysis.

9. Experimental Results and Discussion

The following sections of this research will comprehensively evaluate the suggested LWBC, analysing its suitability and efficiency in IoT applications. When assessing the energy consumption of a cryptographic algorithm compared to other LWBCs, several factors must be considered, including algorithm complexity, operational modes, and hardware optimisation. Lightweight ciphers are specifically designed to maximise computational efficiency while minimising energy usage. Therefore, the energy per bit metric becomes a critical criterion for comparison.

To evaluate the effectiveness of a created cipher, its performance on similar systems can be compared to established ciphers such as PRESENT, PRINT, TEA, RECTANGLE, and PRINT. This comparison can help to determine the cipher's suitability for specific applications and system configurations.

Table 4 compares our proposed lightweight block cipher and well-known alternatives, providing insights into its efficiency and resource usage. This comparison is essential for comprehending the efficacy and potency of our approach about current algorithms. Necessary measurements, such as the size of the encryption key, the size of data blocks, the number of encryption rounds, the structure of the network, the amount of energy consumed per bit (measured in microjoules), the area occupied by the encryption circuitry (measured in gate equivalents or GEs), the amount of memory needed for read-only memory (ROM) in bytes, the time delay per block (measured in cycles), and the rate of data transfer (measured in kilobits per second per kilobyte at 100 MHz), are taken into account. This comparison emphasises each cipher's advantages and compromises, offering a thorough view of the latest advancements in LWBC design. We analysed our suggested cipher, as well as established algorithms such as Piccolo, RECTANGLE, PRINT, PRESENT, PUFFIN, ICEBERG, HIGH, and TEA, to gain a comprehensive grasp of its performance in key features relevant to IoT and comparable applications. This research presents an efficient block cipher tailored explicitly for IoT end devices. The cipher considers the limitations of power, memory, and processor capabilities, which are crucial factors in this context. The evaluation of this encryption and decryption method is systematically divided into two fundamental components: resource allocation, specifically, power consumption, followed by security analysis.

Table 4. Comparison of various resource consumption by various LWBC algorithms.

Algorithms	Key Type (Partial/Full Key)	Block Size	Rounds	Network Structure	Energy (µJ/bit)	Gate Area (GE)	Memory ROM (byte)	Latency (Cycles/block)	Throughput (@100 MHz Kbps/KB)
Proposed Cipher	Partial Key or half key	64	10	SPN	4.50	1450	1408	11,892	180
Piccolo [18,29]	Full key	64	25, 30	GFN	4.80	1136	2654	25,681	237
RECTANGLE [26]	Full key	64	25	SPN	5.96	1787	-	-	246
PRINT [30]	Full key	48	48	SPN	7.54	503	6210	35,161	100
PRESENT [27]	Full key	64	31	SPN	11.77	1570	1562	10,792	200
PUFFIN [54]	Full key	64	32	SPN	19.32	2577	-	1240	200
ICEBERG [31,32]	Full key	64	16	SPN	21.81	5800	-	16,660	400
HIGH [32]	Full key	64	32	ARX + GFN	29.14	3048	1340	-	470
TEA [33,54,55]	Full key	64	64	Fiestel	35.32	3872	1354	9129	194

9.1. Resource Utilisation Analysis

The practical implementation of cryptographic solutions in the context of the IoT depends on efficient resource use, particularly power consumption. This analysis section will comprehensively evaluate the proposed cipher's power efficiency. Given the energy-constrained nature of IoT devices, the power consumption test is not just an indicator of efficiency but also a critical factor in determining the technology's feasibility for real-world applications.

In addition to evaluating power efficiency, this examination encompasses assessments of gate area, throughput, key and block sizes, and the impact on device memory (ROM). However, the primary focus remains on power usage, which aligns with the research's title and underscores the need for energy-efficient cryptographic techniques in IoT systems with limited resources. This methodology draws inspiration from research investigations, such as the survey conducted by Eisenbarth et al. on lightweight cryptographic algorithms [55].

9.1.1. Energy Consumption Analysis

This analysis aims to measure and understand the power and current demands of a lightweight block cipher algorithm when executed on the ESP8266 NodeMCU V3. The Otii Arc Pro will be used for accurate energy measurement.

The Otii Arc device provides essential insights into the energy consumption of the cipher during operation. These findings are helpful for optimising energy efficiency in practical applications. When evaluating the energy usage of cryptographic algorithms, it is crucial to consider various factors that can influence their performance. By carefully analysing these factors and comparing them to established ciphers, researchers and developers can create more efficient and effective lightweight ciphers that meet the demands of modern computing systems. Figure 9 visually represents the interconnection between IoT devices, Otii Arc, and computers. The connection details are already discussed in Section 6.

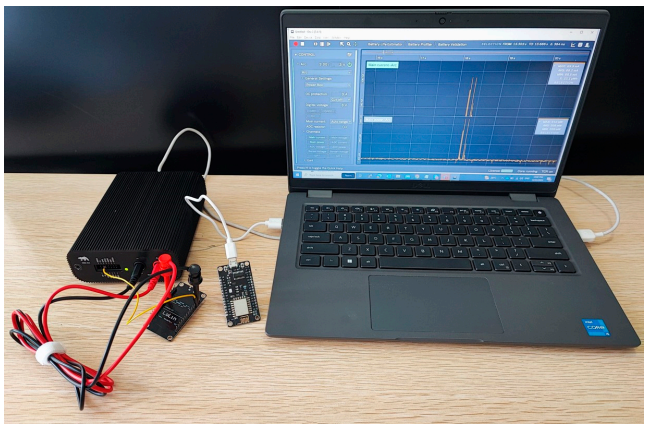

Figure 9. A physical connection between devices while measuring power consumption.

The measurements obtained from Figure 10, using the Otii Arc device, indicate an average power usage of 138.4 milliwatts during encryption and decryption, equivalent to 0.1384 watts. The encryption and decryption procedure involves transforming a 64 bit plaintext to ciphertext and vice versa and is completed in 2.1 milliseconds (equal to 2.1×10^{-3} s). By multiplying the values of power and time, we can determine the overall energy usage, which amounts to 290 microjoules.

Dividing this energy consumption by the number of processed bits (64) yielded an energy efficiency of approximately 4.50 microjoules per bit. This key metric underlines the cipher's suitability for resource-constrained devices, such as IoT endpoints, where energy preservation is critical. It quantitatively measures the cipher's performance in energy-hungry environments, highlighting its potential for practical applications.

An examination of resources utilising the ESP8266 NodeMCU V3 and the Otii Arc Pro, explicitly focusing on power usage, provides valuable insights into the energy efficiency of an LWBC. This research is essential for optimising IoT devices, guaranteeing their efficient operation.

The energy consumption of block ciphers has been a topic of significant interest in recent years, particularly in the context of energy-limited devices such as IoT end devices. In this regard, the power consumption rate of various block ciphers has been measured and expressed in microjoules per bit. Figure 11 illustrates the results of this analysis.

Figure 10. Power consumption measurement by Otii Arc.

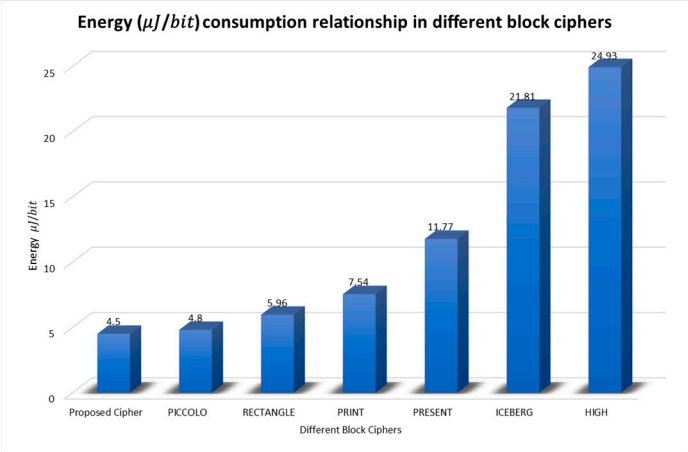

Figure 11. Evaluate various LWBCs' energy consumption.

Our proposed cipher has shown the most efficient design among the ciphers, with a power consumption rate of 4.50 microjoules per bit. This design is superior to the alternatives and provides a promising solution for energy-limited devices. The Piccolo cipher comes in a close second, with an energy efficiency of 4.80 microjoules per bit, which is still competitive. However, the RECTANGLE cipher falls in the middle range with a power demand of 5.96 microjoules per bit.

On the other hand, the PRINT and PRESENT ciphers show relatively high energy consumption levels of 7.54 and 11.77 microjoules per bit, respectively, making them less suitable for energy-limited situations. The ICEBERG and HIGH ciphers exhibit significantly higher power utilisation levels of 21.81 and 29.14 microjoules per bit, respectively. This suggests a substantial increase in power consumption, which could be a critical constraint when using these ciphers in IoT end devices where power efficiency is crucial.

The findings of this study highlight the crucial role of power consumption rate in designing energy-efficient IoT end devices with various block ciphers. Our proposed cipher presents a compelling solution for such scenarios, owing to its highly efficient architecture and low power consumption rate.

9.1.2. Key Type (Full/Partial Key)

We use the 64 bit key to our cipher, ideally suited for IoT devices, striking a balance between security and efficiency. The proposed cipher is a balanced solution between 80 bit and 128 bit ciphers such as Piccolo, RECTANGLE, PRINT, PRESENT, PUFFIN, ICEBERG,

HIGH, and TEA. It may offer a different level of complexity than 128 bit ciphers. We use a middle layer to overcome this restriction and regularly update the key. The middle layer enhances the complexity, while key freshness enhances the resilience of the cipher with the smaller key. A 64 bit key decreases the computational and memory requirements, which are crucial for IoT devices with limited resources. This enhanced efficiency results in reduced power usage for portable IoT devices. A lower key size decreases the memory used, which is valuable for systems with limited ROM and random access memory (RAM). The scalability and versatility of the cipher make it suitable for a wide range of applications, from basic sensors to large IoT systems.

9.1.3. Block Size

Selecting an appropriate block size is crucial in achieving an optimal balance between security and efficiency in cryptographic algorithms. While bits play a vital role, other aspects, such as processing speed and resource usage, should also be considered. Several ciphers, including Piccolo, RECTANGLE, PRESENT, PUFFIN, ICEBERG, HIGH, and TEA, have adopted the 64 bit block size due to its reliable cryptographic capabilities and efficient data processing without overburdening resources. This preference for the 64 bit block size in the industry is a testament to its effectiveness in balancing security and efficiency.

We confidently propose a cipher that aligns with the industry standard of the 64 bit block size. Our cipher provides robust security and optimal performance, making it ideal for the high standards of the IoT industry, where both factors are crucial. The 64 bit block size assures the necessary cryptographic strength to secure data transmissions while ensuring the efficient processing of vast data. In the context of IoT, where billions of devices are connected and data transfer is constant, our cipher provides a dependable and secure solution that meets the industry's demands.

Therefore, selecting an appropriate block size is critical in achieving the optimal balance between security and efficiency. The industry preference for the 64 bit block size is a testament to its effectiveness in meeting these requirements. Our proposed cipher aligns with this industry standard and provides a robust and efficient solution that meets the demands of the IoT industry.

9.1.4. Rounds

The use of traditional LWBCs such as Piccolo, PRESENT, and PUFFIN for security purposes has been widely acknowledged. However, these ciphers rely on multiple rounds (25–31, 31, and 32, respectively) to achieve a desirable level of security. In contrast, our innovative technique achieves the same level of security with only ten rounds, which is remarkable. This approach unlocks unparalleled efficiency by drastically reducing computational requirements and processing time, making it an ideal choice for resource-constrained devices.

While it may be tempting to assume that simplicity implies weakness in security, it is essential to note that our cipher employs an advanced middle layer and dynamic key refreshes to address the limitations of a single round. A multitiered security system enhances intricacy and resilience, protecting against prevalent threats, particularly in IoT devices with limited resources.

Furthermore, our cipher's distinctive architecture makes it a superior choice for optimising efficiency in applications where utilising bits and cycles is crucial. For instance, the cipher can be used in sensor networks to enable rapid communication while consuming minimal resources.

The innovative technique we have developed for LWBCs is a significant milestone in the quest for efficient and secure ciphers. Using a single round to achieve a desirable level of security, coupled with advanced middle-layer techniques and dynamic key refreshes, makes the cipher a robust and efficient choice for resource-constrained devices.

9.1.5. Cipher Architecture

The SPNs have emerged as a popular choice among several architectures used in lightweight ciphers due to their efficient and smart combination of protection. SPNs have been utilised in well-known ciphers like ICEBERG, PUFFIN, PRINT, PRESENT, and RECTANGLE. In resource-constrained environments such as those encountered in military applications, SPNs offer an attractive solution due to their simple deployment and inherent strength in security.

The proposed cipher, which leverages SPN, has been specifically designed to meet the security and performance requirements of soldiers with limited resources. The cipher has been developed to emphasise efficiency, utilising a generalised Feistel network (GFN) to balance security and performance.

To enhance its strength, HIGH combines ARX with GFN. On the other hand, TEA relies on a traditional Feistel network for simplicity. However, in the resource-constrained environment of IoT, SPNs have demonstrated superior performance due to their simple deployment and inherent strength in security.

The proposed cipher has demonstrated remarkable efficiency in the resource-intensive domain of IoT, facilitating secure connectivity while minimising resource consumption. Its SPN architecture offers a balanced trade-off between security and efficiency, making it an attractive solution for resource-constrained environments.

Using the SPN architecture, the proposed cipher offers an efficient and secure solution for resource-constrained environments. Its use of GFN ensures a balance between security and performance, while its inherent security strength makes it an attractive option for IoT applications.

9.1.6. Gate Area (GE)

The gate area (GE) is a crucial parameter for evaluating the hardware efficiency of lightweight block ciphers. It is quantified by the number of basic logic gates (such as two-input NAND gates) required for implementation. Minimising silicon space and power consumption is vital in resource-constrained contexts like IoT devices. A lower GE value signifies a more efficient cipher in terms of area, making it suitable for applications with limited space and energy resources [56].

The proposed cipher for the LWBC gate area is strategically designed to provide a footprint of 1450 GE. It balances compactness and functionality that surpasses several existing ciphers, such as RECTANGLE, PRESENT, PUFFIN, ICEBERG, HIGH, and TEA. This balance makes it a viable option for IoT applications where limited resources and power usage are critical factors.

The proposed cipher offers a smaller hardware size and reduced power usage, which makes it an exceptional choice for IoT applications. Although Piccolo and PRINT may cover a smaller area, the proposed cipher remains strong, providing a competitive advantage when balancing size, strength, and security, which are crucial for IoT applications. This establishes it as a strong competitor for IoT applications where the performance of each gate and the power consumption of every milliwatt are crucial, demonstrating the effectiveness of the proposed cipher in achieving efficiency in several ways, not solely by minimizing size.

Overall, the proposed cipher for the LWBC gate area shows significant promise in compactness, functionality, and security, particularly for IoT applications. Its strategic design and competitive advantage make it a strong contender in the field and support its potential for broader implementation in IoT environments.

9.1.7. ROM

Low-power wireless devices, such as those used in the IoT, have limited resources and require a critical factor for their functionality: read-only memory (ROM) [57]. The amount of ROM used is a crucial factor in determining the efficiency and functionality of these devices. This research proposes a new cipher that stands out for its impressively small ROM size of only 1408 bytes, offering clear benefits over existing counterparts.

The proposed cipher outperforms existing ciphers regarding ROM size, demonstrating a substantial decrease in reliance on ROM compared to Piccolo, which requires a vast 2654 bytes, and PRESENT, which needs a more moderate 1562 bytes. Furthermore, the proposed cipher offers more efficiency improvements than PRINT (1268 bytes) and TEA (1354 bytes). The cipher's small size results from its design, which balances efficiency and functionality, making it an attractive option for IoT applications with limited resources.

The proposed cipher's shallow ROM requirement makes it a promising candidate for IoT applications where each byte is significant. Its potential to relieve memory constraints while guaranteeing solid cryptographic security makes it suitable for diverse IoT applications. In conclusion, the proposed cipher offers a solution to the challenge of ROM size in LWBCs, making it a valuable contribution to the field of cryptography.

9.1.8. Latency

Table 3 compares the latency, expressed in cycles per block, for different LWBCs, including the cipher we proposed. The latency of our cipher is 11,892 cycles per block, which gives it a competitive advantage compared to most of the mentioned algorithms, particularly ICEBERG (16,600 cycles/block), Piccolo (25,681 cycles/block), and PRINT (35,161 cycles/block). This suggests that our cipher is more efficient in terms of cycle usage. Nevertheless, it exhibits more delay than PRESENT (10,792 cycles/block) and TEA (9129 cycles/block). While the cipher might not be the fastest in absolute terms, it certainly does a commendable job when considering other crucial factors for IoT devices, such as security, battery consumption, and implementation size. In real-world applications for IoT end devices, balancing security and efficiency is crucial, and these concerns are often more significant. Our cipher has a reasonably short delay and is likely designed to be efficient in other aspects. This makes it a potentially better option for specific IoT applications requiring a trade-off between speed and other performance measures.

9.1.9. Throughput

Our proposed cipher achieves a data transfer rate of 180 kilobits per second per kilobyte at a frequency of 100 megahertz, which exceeds the performance of PRINT. However, it is positioned among several other data transfer rates in the field of LWBC throughput. Piccolo, RECTANGLE, and other well-established counterparts dominate the field, demonstrating exceptional velocity. Nevertheless, our approach is particularly well-suited for IoT devices with limited resources, where a moderate level of data transfer is usually adequate because the tasks involved are not highly data intensive. Our method achieves a promising equilibrium when prioritising maximal throughput may not result in optimal real-world efficiency. By demonstrating superior performance in critical aspects such as power efficiency, data protection, and compact design, it can become the preferred option for IoT applications requiring a comprehensive cryptographic solution. Ultimately, the most suitable candidate depends on the overall speed and complex interaction of performance measurements that align with the application's requirements.

9.2. Security Analysis

Assessing the security of a suggested cipher is a critical aspect that necessitates extensive research on resource utilisation. In the IoT domain, the security of cryptographic implementations is of utmost importance as devices face increasingly sophisticated cyberattacks. Consequently, a thorough analysis encompassing a range of tests is crucial to evaluate the cipher's resistance against prevalent cryptographic attacks such as differential and linear cryptanalysis, chosen plaintext attacks, and known plaintext assaults. The cipher's resilience against these assaults is fundamental in ensuring the integrity and confidentiality of data in IoT applications.

This subsection presents an in-depth analysis of the security features of our proposed LWBC, which is explicitly designed for IoT end devices. Our primary focus is to evaluate

the cipher's ability to withstand brute force, man-in-the-middle (MitM), and side-channel attacks, which are critical for ensuring robust data security in IoT environments.

9.2.1. Brute Force Attack

The security of a cipher is of utmost importance in ensuring the confidentiality of sensitive information. The exponential growth of the key space significantly enhances the cipher's security by protecting against brute-force assaults. As the size of the key space increases, the number of potential key combinations also increases.

To assess the probable time needed for a brute force attack to breach a cipher, two crucial factors must be considered: the size of the key space and the speed at which an attacker can test different keys. Assuming that an attacker had a machine capable of trying 1 billion (10 to the ninth) keys per second, which is a reasonable estimate for modern high-power systems, the average time required to obtain the appropriate key would involve examining half of the 64 bit key space, which is around 2 to the 63 keys.

Based on these assumptions, the calculations indicate that finding the proper key would take around 292 years. However, it is essential to note that this estimate is based on ideal conditions, and the time needed could be much longer. Furthermore, the protocol regularly updates encryption keys, making it even more difficult for an attacker to decipher the information.

Protecting against brute force attacks is significant in the real world, especially when dealing with sensitive information. Current technology must improve the time needed to launch a brute-force attack on a 64 bit cipher. Hence, it is essential to have a robust and secure encryption mechanism in place to safeguard against potential attacks.

9.2.2. Man-in-the-Middle Attack

An MitM attack is a cyberattack in which an unauthorised individual intercepts, decrypts, or alters encrypted data delivered through a network. The decryption of intercepted data usually requires the attacker to determine the encryption key, which can be time-consuming and computationally demanding. In some cases, the process can take several years to complete, especially in the context of brute-force attacks. The viability of this strategy is dependent on the computational resources the attacker has at their disposal.

We conducted targeted experiments to evaluate the resistance of our proposed LWBC against MitM attacks. One particular test involved modifying the cipher text produced by our proposed cipher. We added an extra binary bit to the cipher text obtained from the "Hello World" input. After decrypting, the modified cipher text produced a result that, although fully deciphered, contained nonsensical or garbled information. The cipher's susceptibility to even minor changes in the cipher text is desirable for preventing man-in-the-middle attacks involving data tampering.

In another experiment, we replaced a '1' in the cipher text with a binary '0'. This seemingly insignificant modification led to a substantially different decrypted outcome, illustrating our LWBC's resilience against discreet attempts to manipulate encrypted messages. Such trials are crucial for evaluating the cipher's integrity and capacity to preserve data confidentiality in the face of MitM attack scenarios.

Overall, the results of our experiments suggest that our proposed LWBC is resistant to MitM attacks. The cipher's susceptibility to even minor changes in the cipher text makes it challenging for attackers to manipulate encrypted messages without being detected. These findings support using our proposed LWBC for secure communication over networks.

9.2.3. Side-Channel Attack

During cryptographic operations, side-channel attacks (SCAs) exploit physical information leaks, such as timing, power consumption, and electromagnetic emissions. In resource-constrained IoT environments, where devices may lack advanced countermeasures, lightweight block ciphers are particularly vulnerable to SCAs. Our LWBC addresses

these vulnerabilities by employing several strategies, including key randomisation, structural complexity, and operational techniques to obfuscate side-channel signatures.

a. Key Randomisation for Enhanced Unpredictability

A primary defence mechanism against SCAs in our LWBC is its key randomisation approach. For every encryption cycle, a fresh 64 bit key is derived from a pool of 32 bit subkeys, creating a unique key instance for each operation. This randomisation increases entropy, as the keys are drawn from an order list of diverse devices, introducing a layer of unpredictability. Consequently, attackers cannot rely on static key correlations, as they face different keys per encryption cycle, making it challenging to exploit observed power or timing characteristics across cycles.

- Preventing key guessing: the frequent key variation ensures that side-channel information related to a particular encryption cycle has limited value, as it becomes infeasible for attackers to predict or reuse key-based patterns.
- Key isolation across cycles: selecting a fresh key for each cycle limits any cross-cycle correlation, thus reducing the effectiveness of correlation-based side-channel analysis (e.g., differential power analysis, DPA) that relies on consistent key information.

b. Robust S-box and P-box Design for Enhanced Confusion and Diffusion

Our cipher's S-box and P-box structures are designed to maximise confusion and diffusion, effectively obfuscating any direct relationship between the input, output, and intermediate states. The S-box, a nonlinear substitution function, generates high nonlinearity, thereby complicating the identification of side-channel leaks through linear analysis.

- High nonlinearity: the high nonlinearity of the S-boxes ensures that even minor input changes cause substantial output changes, disrupting the potential for simple power analysis (SPA) and other direct SCAs.
- Permutation for diffusion: the P-box permutations disperse the bits across different segments, minimising leakage points and making it challenging for attackers to correlate observed power usage or timing data with specific input–output pairs.

c. Iterative Processing with XOR Operations and Data Chunking

The iterative nature of LWBCs, involving multiple encryption rounds with XOR operations and data chunking, introduces dynamic transformations in each encryption phase. Each XOR operation disrupts the intermediate values of data blocks, complicating the attackers' ability to analyse and predict the internal states based on side-channel information.

- Randomised intermediate states: by performing repeated XORs with key bits and splitting data into chunks, our cipher creates randomised intermediate states that reduce consistency in side-channel signatures, thus hampering the effectiveness of DPA attacks.
- Variable round outputs: the iterative rounds in LWBCs modify power consumption patterns and timing behaviour for each round, creating variability in side-channel emissions that prevent precise analysis across cycles.

d. Masking and Noise Injection for Increased Ambiguity

While inherent to the cipher's structural properties rather than explicit masking techniques, the design of LWBCs incorporates elements akin to random noise in side-channel outputs. This is achieved through multiple data transformation and key-mixing rounds, effectively diluting any identifiable power or timing patterns.

- Natural noise and ambiguity: the data transformation and XOR operations within each round generate inherent variability in power consumption and electromagnetic emissions. This masks the operational patterns, making it difficult for attackers to distinguish between meaningful data and noise.

- Adaptive complexity: The variation in bitwise transformations across rounds naturally introduces signal noise, thus mitigating differential side-channel analysis where attackers attempt to deduce secrets by analysing the differences in side-channel data.

e. Temporal Obfuscation through Modified Side-Channel Signatures

The cipher's iterative design, characterised by frequent modifications in each encryption stage, disrupts side-channel signatures, making it difficult for attackers to correlate observed patterns with specific stages of the encryption process.

Multistage modifications: every round in the LWBC performs unique bitwise operations that significantly alter the data flow, effectively breaking the temporal correlation necessary for SCAs.

Dynamic timing patterns: by introducing slight variations in processing time across rounds, our cipher creates inconsistent timing profiles, which serve as an additional layer of protection against timing attacks, where attackers leverage execution timing data to deduce key information.

f. Balancing Lightweight Design with SCA-Resistance

While achieving complete immunity to side-channel attacks remains challenging, our LWBC incorporates these design principles while maintaining a lightweight structure suitable for IoT devices. By optimising key randomisation, nonlinear transformations, and multistage processing, our LWBC ensures that side-channel protection does not compromise performance or exceed the resource constraints of IoT environments.

In summary, the proposed LWBC's combination of key randomisation, robust S-box and P-box configurations, iterative XOR-based transformations, and natural noise generation offers a multilayered defence against side-channel attacks. These design choices balance the need for efficient cryptographic operations with effective SCA resistance, making the LWBC suitable for securing IoT devices against physical data leakage while preserving lightweight operation. This enhanced resilience is particularly beneficial in heterogeneous IoT ecosystems where devices may lack additional hardware-based security support, as the cipher's design inherently mitigates key SCA vectors.

9.3. Results Summary

The block cipher we propose demonstrates remarkable cryptographic robustness. The vast 64 bit key space makes brute-force attacks impossible, necessitating an extremely long time for decryption, even in the most favourable circumstances. Periodic key upgrades significantly improve security. The effectiveness of robust defences against man-in-the-middle attacks is proved by studies in which even little adjustments to the ciphertext make the data unintelligible, ensuring the integrity and confidentiality of the information. Furthermore, the cipher integrates advanced countermeasures to mitigate side-channel attacks, a significant problem in the IoT environment. The features contributing to increased unpredictability and hamper side-channel data analysis are dynamic key generation per iteration, a sophisticated S-box and P-box architecture, and iterative processing. The complex security measures make the cipher an excellent option for protecting sensitive data in limited-resource contexts like IoT devices.

The suggested LWBC is highly appropriate for IoT devices due to its extraordinary power consumption efficiency of only 4.5 μJ/bit. The low energy need of this technology is a crucial advantage in IoT situations.

9.4. Leveraging the Proposed LWBC in Existing Mobile Applications

The proposed LWBC can be leveraged in existing mobile applications to enhance both security and energy efficiency in the following ways:

- Offloading computational workloads to smartphones: similar to the approach described in "Smartphone-assisted energy-efficient data communication," our LWBC can be deployed in mobile applications where smartphones handle the bulk of cryptographic computation. Wearable or IoT devices transmit minimally processed data to

a smartphone, which performs the encryption using LWBC. This allows low-power devices to conserve energy while benefiting from the robust encryption provided by the LWBC on the smartphone, where computational resources are less constrained.

- Optimising energy consumption through lightweight cipher characteristics: the LWBC's lightweight design minimises processing load and memory usage, making it suitable for mobile and wearable devices that communicate frequently. By integrating the LWBC, existing mobile applications can secure data transmissions from wearables without significant additional energy consumption, extending battery life in both the wearable device and the smartphone.
- Compatibility with energy-sensitive data transfer protocols: the LWBC is adaptable for secure, energy-efficient data communication protocols commonly used in mobile applications, such as Bluetooth Low Energy (BLE) and Wi-Fi Direct. These protocols, often used to link wearables with smartphones, can leverage the LWBC to encrypt data before transmission, ensuring secure communication without the overhead of more resource-intensive cryptographic methods.
- Modular integration: our proposed method's lightweight structure allows it to be integrated as a modular encryption component within mobile applications, facilitating retrofitting into existing software with minimal modifications. This modular approach aligns well with applications focused on smartphone-assisted data handling, where the security layer can be optimised independently.

By adapting our LWBC within the data-handling architecture of mobile applications, it is feasible to achieve both security and energy efficiency in systems that support wearable devices and other low-power IoT peripherals.

10. Conclusions

The comprehensive investigation into the proposed lightweight block cipher (LWBC) has unveiled a compelling cryptographic solution specifically tailored for the intricate landscape of Internet of Things (IoT) applications. This study offers a thorough analysis of the LWBC's power consumption and overall efficiency, complemented by a meticulous exploration of its security features through rigorous examination. Notably, the LWBC demonstrates exceptional power efficiency, with a minimal consumption rate of 4.5 microjoules per bit, significantly extending the operational lifespan of IoT device batteries. This remarkable efficiency renders the cipher an ideal candidate for energy-sensitive environments, such as those utilising energy-harvesting techniques or operating under low-power conditions. Moreover, the LWBC's design—featuring a 64 bit key and a single-round architecture with dynamic key updates—displays resilience against common cryptographic attacks, underscoring its commitment to robust security.

The security analysis further affirms the LWBC's credibility in the domain of cryptography. Its expansive 64 bit key space fortifies resistance to brute-force attacks, rendering decryption via exhaustive key search a challenging endeavour. Additionally, the cipher exhibits notable resilience against man-in-the-middle (MitM) attacks, as even minor alterations to the ciphertext yield unintelligible deciphered data, thus ensuring both the integrity and confidentiality of the information. The LWBC's heightened resistance to side-channel attacks is achieved through dynamic key generation and a sophisticated S-box and P-box architecture, effectively mitigating vulnerabilities associated with physical data execution. Overall, the LWBC achieves a balanced approach to key dimensions such as key and block size, latency, and throughput, thereby positioning itself as a competitive solution within the resource-restricted environments typical of IoT applications. Its holistic strengths in power optimisation, security robustness, and efficient resource utilisation mark it as a pioneering development in lightweight cryptography, with the potential to significantly enhance the evolving field of IoT security.

Author Contributions: Conceptualization, M.R. and Q.M.; Methodology, M.R.; Validation, M.R. and R.I.; Formal analysis, M.R.; Investigation, Q.M.; Writing—original draft, M.R.; Writing—review & editing, Q.M. and R.I.; Visualization, M.R.; Supervision, Q.M. and R.I. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Cyber Security Cooperative Research Centre (CSCRC) Australia, Project #P23-00299. The APC was waived by MDPI.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding authors.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Zhong, Y.; Gu, J. Lightweight block ciphers for resource-constrained environments: A comprehensive survey. *Future Gener. Comput. Syst.* **2024**, *157*, 288–302. [CrossRef]
2. Rana, M.; Mamun, Q.; Islam, R. Lightweight cryptography in IoT networks: A survey. *Future Gener. Comput. Syst.* **2022**, *129*, 77–89. [CrossRef]
3. Latif, S.A.; Wen, F.B.X.; Iwendi, C.; Li-Li, F.W.; Mohsin, S.M.; Han, Z.; Band, S.S. AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. *Comput. Commun.* **2022**, *181*, 274–283.
4. Atlam, H.F.; Alenezi, A.; Alharthi, A.; Walters, R.J.; Wills, G.B. Integration of cloud computing with internet of things: Challenges and open issues. In Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, UK, 21–23 June 2017; pp. 670–675.
5. Nižetić, S.; Šolić, P.; Gonzalez-De, D.L.D.I.; Patrono, L. Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *J. Clean. Prod.* **2020**, *274*, 122877. [CrossRef]
6. Rana, M.; Mamun, Q.; Islam, R. A block cipher for resource-constrained IoT devices. *World Acad. Sci. Eng. Technol.* **2023**, *17*, 266–271.
7. Rana, M.; Mamun, Q.; Islam, R. An S-box design using irreducible polynomial with affine transformation for lightweight cipher. In Proceedings of the Quality, Reliability, Security and Robustness in Heterogeneous Systems: 17th EAI International Conference, QShine 2021, Virtual Event, 29–30 November 2021; Proceedings 17; Springer International Publishing: Berlin/Heidelberg, Germany, 2017; pp. 214–227.
8. Rana, M.; Mamun, Q.; Islam, R. P-Box Design in Lightweight Block Ciphers: Leveraging Nonlinear Feedback Shift Registers. In Proceedings of the 2024 IEEE Wireless Communications and Networking Conference (WCNC), Dubai, United Arab Emirates, 21–24 April 2024; pp. 1–8.
9. Rana, M.; Mamun, Q.; Islam, R. Enhancing IoT security: An innovative key management system for lightweight block ciphers. *Sensors* **2023**, *23*, 7678. [CrossRef]
10. Caforio, A.; Balli, F.; Banik, S.; Regazzoni, F. A deeper look at the energy consumption of lightweight block ciphers. In Proceedings of the 2021 Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France, 1–5 February 2021; pp. 170–175.
11. Zitouni, N.; Sedrati, M.; Behaz, A. LightWeight energy-efficient Block Cipher based on DNA cryptography to secure data in internet of medical things devices. *Int. J. Inf. Technol.* **2024**, *16*, 967–977. [CrossRef]
12. Fan, R.; Cui, Y.; Chen, Q.; Wang, M.; Zhang, Y.; Zheng, W.; Li, Z. MAICC: A Lightweight Many-core Architecture with In-Cache Computing for Multi-DNN Parallel Inference. In Proceedings of the 56th Annual IEEE/ACM International Symposium on Microarchitecture, Toronto, ON, Canada, 28 October 2023; pp. 411–423.
13. Yang, K.; Shi, Y.; Ding, Z. Data shuffling in wireless distributed computing via low-rank optimization. *IEEE Trans. Signal Process.* **2019**, *67*, 3087–3099. [CrossRef]
14. Cazorla, M.; Marquet, K.; Minier, M. Survey and benchmark of lightweight block ciphers for wireless sensor networks. In Proceedings of the 2013 International Conference on Security and Cryptography (SECRYPT), Reykjavik, Iceland, 29–31 July 2013; pp. 1–6.
15. Mohd, B.J.; Hayajneh, T. Lightweight block ciphers for IoT: Energy optimization and survivability techniques. *IEEE Access* **2018**, *6*, 35966–35978.
16. Mishra, R.; Okade, M.; Mahapatra, K. FPGA based High Throughput Substitution Box Architectures for Lightweight Block Ciphers. In Proceedings of the 2022 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA), Bangalore, Karnataka, 5–6 September 2024; pp. 1–7.
17. Fan, T.; Li, L.; Wei, Y.; Pasalic, E. Differential cryptanalysis of full-round ANU-II ultra-lightweight block cipher. *Int. J. Distrib. Sens. Netw.* **2022**, *18*, 15501329221119398. [CrossRef]
18. Mhaouch, A.; Elhamzi, W.; Abdelali, A.B.; Atri, M. Optimized Piccolo lightweight block cipher: Area efficient implementation. *Trait. Du Signal* **2022**, *39*, 805. [CrossRef]

19. Balasubramanian, N.; Balasubramanian, A.; Venkataramani, A. Energy consumption in mobile phones: A measurement study and implications for network applications. In Proceedings of the 9th ACM SIGCOMM Conference on Internet Measurement, Chicago, IL, USA, 4–6 November 2009; pp. 280–293.
20. Shang, G.; Zhe, P.; Bin, X.; Yubo, S. Secure and energy efficient prefetching design for smartphones. In Proceedings of the 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 22–27 May 2016; pp. 1–6.
21. Yan, M.; Chan, C.A.; Gygax, A.F.; Yan, J.; Campbell, L.; Nirmalathas, A.; Leckie, C. Modeling the total energy consumption of mobile network services and applications. *Energies* **2019**, *12*, 184. [CrossRef]
22. Nadeem, A.; Javed, M.Y. A performance comparison of data encryption algorithms. In Proceedings of the 2005 International Conference on Information and Communication Technologies, Hokkaido, Japan, 3–5 August 2005; pp. 84–89.
23. Prasithsangaree, P.; Krishnamurthy, P. Analysis of energy consumption of RC4 and AES algorithms in wireless LANs. In Proceedings of the GLOBECOM'03. IEEE Global Telecommunications Conference (IEEE Cat. No. 03CH37489), San Francisco, CA, USA, 1–5 December 2003; Volume 3, pp. 1445–1449.
24. Grossschadl, J.; Tillich, S.; Rechberger, C.; Hofmann, M.; Medwed, M. Energy evaluation of software implementa-1372 tions of block ciphers under memory constraints. In Proceedings of the 2007 Design, Automation & Test in Europe Conference & Exhibition, Nice, France, 16–20 April 2007; pp. 1–6.
25. Hager, C.T.; Midkiff, S.F.; Park, J.M.; Martin, T.L. Performance and energy efficiency of block ciphers in personal digital assistants. In Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications, Washington DC, USA, 17–21 March 2025; pp. 127–136.
26. Zhang, W.; Bao, Z.; Lin, D.; Rijmen, V.; Yang, B.; Verbauwhede, I. RECTANGLE: A bit-slice lightweight block cipher suitable for multiple platforms. *IACR Cryptol. eprint Arch.* **2014**. [CrossRef]
27. Bogdanov, A.; Knudsen, L.R.; Leander, G.; Paar, C.; Poschmann, A.; Robshaw, M.J.; Seurin, Y.; Vikkelsoe, C. PRESENT: An ultra-lightweight block cipher. In Proceedings of the Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, 10–13 September 2007; Proceedings 9; Springer: Berlin/Heidelberg, Germany, 2007; pp. 450–466.
28. Hasan, H.; Ali, G.; Elmedany, W.; Balakrishna, C. Lightweight encryption algorithms for internet of things: A review on security and performance aspects. In Proceedings of the 2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Sakheer, Bahrain, 20–21 November 2022; pp. 239–244. [CrossRef]
29. Shibutani, K.; Isobe, T.; Hiwatari, H.; Mitsuda, A.; Akishita, T.; Shirai, T. Piccolo: An ultra-lightweight blockcipher. In Proceedings of the Cryptographic Hardware and Embedded Systems–CHES 2011: 13th International Workshop, Nara, Japan, 28 September–1 October 2011; Proceedings 13; Springer: Berlin/Heidelberg, Germany, 2011; pp. 342–357.
30. Knudsen, L.; Leander, G.; Poschmann, A.; Robshaw, M.J. PRINT cipher: A block cipher for IC-printing. In Proceedings of the Crypto-1391 Graphic Hardware and Embedded Systems, CHES 2010: 12th International Workshop, Santa Barbara, CA, USA, 17–20 August 2010; Proceedings 12; Springer: Berlin/Heidelberg, Germany, 2010; pp. 16–32.
31. Sun, Y.; Wang, M.; Jiang, S.; Sun, Q. Differential cryptanalysis of reduced-round ICEBERG. In Proceedings of the Cryptology-1394 AFRICACRYPT 2012: 5th International Conference on Cryptology in Africa, Ifrance, Morocco, 10–12 July 2012; Proceedings 5; Springer: Berlin/Heidelberg, Germany, 2012; pp. 155–171.
32. Cheng, H.; Heys, H.M. Compact ASIC implementation of the ICEBERG block cipher with concurrent error detection. In Proceedings of the 2008 IEEE International Symposium on Circuits and Systems (ISCAS), Seattle, WA, USA, 18–21 May 2008; pp. 2921–2924.
33. Hong, D.; Sung, J.; Hong, S.; Lim, J.; Lee, S.; Koo, B.S.; Lee, C.; Chang, D.; Lee, J.; Jeong, K.; et al. HIGHT: A new block cipher suitable for low-resource device. In Proceedings of the Cryptographic Hardware and Embedded Systems-CHES 2006: 8th International Workshop, Yokohama, Japan, 10–13 October 2006; Proceedings 8; Springer: Berlin/Heidelberg, Germany, 2006; pp. 46–59.
34. Mishra, Z.; Acharya, B. High throughput novel architectures of TEA family for high speed IoT and RFID applications. *J. Inf. Secur. Appl.* **2021**, *61*, 102906. [CrossRef]
35. Rivest, R.L. The RC5 encryption algorithm. In *International Workshop on Fast Software Encryption*; Springer: Berlin/Heidelberg, Germany, 1994; pp. 86–96.
36. Sun, M.; Xu, X.; Huang, Y.; Wu, Q.; Tao, X.; Zhang, P. Resource management for computation offloading in D2D-aided wireless powered mobile-edge computing networks. *IEEE Internet Things J.* **2020**, *8*, 8005–8020. [CrossRef]
37. Ye, W.; Vijaykrishnan, N.; Kandemir, M.; Irwin, M.J. The design and use of simplepower: A cycle-accurate energy estimation tool. In Proceedings of the 37th Annual Design Automation Conference, Los Angeles, CA, USA, 5–9 June 2000; pp. 340–345.
38. Brooks, D.; Tiwari, V.; Martonosi, M. Wattch: A framework for architectural-level power analysis and optimizations. *ACM SIGARCH Comput. Archit. News* **2000**, *28*, 83–94. [CrossRef]
39. Mishra, P.; Mamidipaka, M.; Dutt, N. Processor-memory coexploration using an architecture description language. *ACM Trans. Embed. Comput. Syst.* **2004**, *3*, 140–162.
40. Sinha, A.; Chandrakasan, A.P. Jouletrack: A web based tool for software energy profiling. In Proceedings of the 38th Annual Design Automation Conference, Las Vegas, NV, USA, 18–22 June 2001; pp. 220–225.
41. Kanitkar, H. Subthreshold Circuits: Design, Implementation and Application. Ph.D. Thesis, Rochester Institute of Technology, Rochester, NY, USA, 2008.

42. Austin, T.; Larson, E.; Ernst, D. SimpleScalar: An infrastructure for computer system modeling. *Computer* **2002**, *35*, 59–67. [CrossRef]
43. Pathak, A.; Hu, Y.C.; Zhang, M. Where is the energy spent inside my app? Fine Grained Energy Accounting on Smartphones with Eprof. In Proceedings of the 7th ACM European Conference on Computer Systems, Bern, Switzerland, 10–13 April 2012; pp. 29–42.
44. Huang, J.; Qian, F.; Gerber, A.; Mao, Z.M.; Sen, S.; Spatscheck, O. A close examination of performance and powercharacteristics of 4G LTE networks. In Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services, Ambleside, UK, 25–29 June 2012; pp. 225–238.
45. Zhang, L.; Tiwana, B.; Qian, Z.; Wang, Z.; Dick, R.P.; Mao, Z.M.; Yang, L. Accurate online power estimation and automatic battery behavior based power model generation for smartphones. In Proceedings of the Eighth IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis, New York, NY, USA, 24–29 October 2010; pp. 105–114.
46. Carroll, A.; Heiser, G. An analysis of power consumption in a smartphone. In Proceedings of the 2010 USENIX Annual Technical Conference (USENIX ATC 10), Boston, MA, USA, 23-25 June 2010.
47. Fitzek, F.H.; Reichert, F. (Eds.) *Mobile Phone Programming: And Its Application to Wireless Networking*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2007.
48. Creus, G.B.; Kuulusa, M. Optimizing mobile software with built-in power profiling. In *Mobile Phone Programming: Application to Wireless Networking*; Springer: Dordrecht, The Netherlands, 2007; pp. 449–462.
49. Nie, T.; Zhou, L.; Lu, Z.M. Power evaluation methods for data encryption algorithms. *IET Softw.* **2014**, *8*, 12–18. [CrossRef]
50. Razaq, A.; Alhamzi, G.; Abbas, S.; Ahmad, M.; Razzaque, A. Secure communication through reliable S-box design: A proposed approach using coset graphs and matrix operations. *Heliyon* **2023**, *9*, e15902. [CrossRef]
51. Kashyap, M.; Sharma, V.; Gupta, N. Taking MQTT and NodeMcu to IOT: Communication in Internet of Things. *Procedia Comput. Sci.* **2018**, *132*, 1611–1618. [CrossRef]
52. Arduino. "Arduino Esp8266 Nodemcu v3" Arduino. Available online: https://www.arduino.cc/ (accessed on 2 February 2024).
53. Qoitech AB. Extend Battery Life. Deliver Quality. Available online: https://www.qoitech.com/ (accessed on 2 February 2024).
54. Cheng, H.; Heys, H.M.; Wang, C. Puffin: A novel compact block cipher targeted to embedded digital systems. In Proceedings of the 2008 11th EUROMICRO Conference on Digital System Design Architectures, Methods and Tools, Parma, Italy, 3–5 September 2008; pp. 383–390.
55. Ragupathy, S.; Mythili, T. Energy optimized simon lightweight security algorithm for internet of medical things (IoMT). *Int. J. Innov. Technol. Explor. Eng.* **2019**, *8*, 1–7.
56. Eisenbarth, T.; Kumar, S.; Paar, C.; Poschmann, A.; Uhsadel, L. A survey of lightweight-cryptography implementations. *IEEE Des. Test Comput.* **2007**, *24*, 522–533. [CrossRef]
57. Hatzivasilis, G.; Fysarakis, K.; Papaefstathiou, I.; Manifavas, C. A review of lightweight block ciphers. *J. Cryptogr. Eng.* **2018**, *8*, 141–184. [CrossRef]