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

Muhammad Rana *, Quazi Mamun , Rafiqul Islam

Posted Date: 10 October 2024

doi: 10.20944/preprints202410.0769.v1

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

 doi:10.20944/preprints202410.0769.v1

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 Wagga, NSW 2678, Australia
* Correspondence: mmrana_au@yahoo.com

Abstract: This research paper presents a detailed analysis of a Lightweight Block Cipher's power consumption and security features (LWBC), 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

1. Introduction

Despite its potential, significant challenges must be addressed to successfully implement the Internet of Things (IoT) [1]. These challenges primarily relate to the energy efficiency and security of IoT devices [2]. Researchers have proposed lightweight cryptography as a promising solution to address these issues. This cryptographic approach is specifically designed for IoT applications and aims to balance safety, performance, and energy efficiency. Doing so may facilitate the adoption and expansion of future IoT technologies.

Over the past few years, our research team has been engaged in designing a lightweight block cipher (LWBC) [3] and its constituent components, namely the substitution box (S-Box) [4], permutation box (P-Box) [5], and Key Management Field [6]. These components were tested individually to assess their performance. Currently, our research is focused on investigating the power consumption of the proposed LWBC by integrating all the components together and then comparing the proposed Cipher with other existing lightweight ciphers.

The objective of this study is to evaluate the energy efficiency of the proposed cipher under varying operational circumstances. Specifically, we seek to quantify the power consumption of the cipher and analyse its performance under different operational scenarios. The results of this investigation will provide valuable insights into the energy efficiency of the proposed cipher and its 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, the 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

 doi:10.20944/preprints202410.0769.v1

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 examining the power consumption, use of other resources, and security aspects of LWBCs. The key contributions of this study are as follows:

- Created exclusively for IoT applications, this technology improves security while maximising energy efficiency.
- Exhibits exceptional energy efficiency per bit compared to other LWBCs, highlighting its suitability for energy-constrained IoT devices.
- The suggested cipher evaluates using essential criteria such as power efficiency, key/block size, rounds, architecture, gate area, ROM, latency, and throughput. This evaluation confirmed that the cipher is an up-and-coming cryptographic solution for applications with limited energy and resources.
- Qoitech Otii Arc was employed to quantify energy usage accurately, utilising the shunt resistor methodology for a systematic study.
- Attains an ideal balance between the effectiveness of security measures and energy conservation, promoting the widespread use of secure IoT technology.

The subsequent sections of this paper are organised as follows: Section 2 establishes the foundation by conducting a comprehensive examination of the existing literature, and Section 3 investigates the currently available lightweight block ciphers. Section 4 presents our rigorous technique for measuring the power usage in the proposed LWBC, followed by a thorough discussion in Section 5. The experimental setup is explained in Section 6, followed by a detailed analysis of the results and a discussion of resource utilisation and security in Section 7. Finally, Section 8 concludes the paper with critical findings and future research directions for power consumption in LWBCs.

2. 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.

2.1. Features to Consider for pOwer Consumption Analysis of LWBC

Power consumption analysis for LWBCs has gained considerable attention in resource-constrained environments [7]. 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:

 doi:10.20944/preprints202410.0769.v1

Firstly, cipher overhead should be examined to evaluate the additional overhead introduced by the LWBC, such as message expansion or extra rounds of computation. Minimising unnecessary protocol overhead while maintaining the cipher's security is essential for achieving energy efficiency [8].

Secondly, it is essential to investigate how much the LWBC supports parallelisation and piping. These features can leverage multi-core architectures, reducing execution time and energy consumption [9].

Thirdly, Memory Usage should be evaluated to optimise memory requirements, including key storage and data structures. This optimisation minimises power consumption, particularly on devices with limited memory resources [10].

Fourthly, Energy-Aware Cipher Design should be explored to identify LWBCs designed with energy efficiency in mind. Some ciphers may incorporate features to adapt dynamically to available energy resources or adjust their behaviour based on power conditions [11].

Fifthly, Quantitative Metrics should be utilised to measure and compare the power consumption of different LWBCs. These metrics include energy per encryption or energy per bit, providing a concrete basis for assessing the efficiency [12].

Finally, Real-world Testing should be conducted on target devices to observe the actual power consumption of the LWBC in practical scenarios. Accounting for communication delays, idle times, and varying workloads provides insights into real-world energy efficiency.

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.

2.2. 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 [13].

Cryptographic Security of 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 [14].

Serial Hardware Architectures for 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 [15].

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 [16]: 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 [17,18]: 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 [17] is thoroughly assessed in these tests, comprehensively evaluating four key metrics: runtime, workload, throughput, and power consumption. Using a UPS

 doi:10.20944/preprints202410.0769.v1

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 [19]: 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 LWBC that were designed considering the abovementioned discussions.

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

This section discusses several LWBCs that have been compared with our proposed cipher [20]. 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 [21]: 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 1467GE 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 [22]: The PRESENT cipher, which meets lightweight conditions, significantly advances LWBCs. It has been standardised in ISO/IEC 29192. 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 1030GE for its execution. Software solutions exhibit a condensed code size and provide excellent performance on microcontrollers. Nevertheless, it is susceptible to side-channel, related-key, biclique, and differential attacks, particularly on variants with fewer rounds.

Piccolo [23]: 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 432GE. An additional 60 gate area (60GE) 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 [24]: 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 402GE, as well as EPC encryption, specifically PRINTcipher-96 and 726GE, 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 [25]: 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 8 rounds. Modern ciphers employ this structure to achieve efficient encryption and decoding at a low cost.

HIGHT [26]: 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

 doi:10.20944/preprints202410.0769.v1

hardware version requires a 2608GE for a data transfer rate of 188Kbps. 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.

4. 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 evaluation for in-depth analysis of individual components. Every method has distinct benefits that cater to specific research objectives and limitations in available resources. An in-depth analysis of all three aspects provides a thorough comprehension of the algorithm's performance characteristics, which is essential for optimising and implementing it in instances with limited resources.

4.1. 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 [27], is a specialised tool used 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 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).

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

Ye et al. [28] presented 'SimplePower,' 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. [29] 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.

 doi:10.20944/preprints202410.0769.v1

Furthermore, the model incorporates an activity component (α) that varies between 0 and 1 represents 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 Brooks et al., 'Wattch' provides a swifter, more precise alternative than currently available power measurement instruments.

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

Sinha and Chandrakasan [30] created 'JouleTrack,' 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.

$$P_{tot} = P_{dyn} + P_{stat} = C_L V_{dd}^2 f + V_{dd} I_{leak} \tag{3}$$

SimpleScalar, as highlighted by Naik and Wei [31], 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.

4.2. 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 [32,33]. Nevertheless, the method's dependence on regular usage fails to consider the varying workloads and power states of devices. This could lead to distorted outcomes due to background processes and the absence of accounting for battery degradation and non-linear discharge characteristics [34,35]. 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.

4.3. External Evaluation

The third category comprises techniques that utilise instruments and electronic equipment to establish a specialised measurement system. The approach is categorised 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 [36]. 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

 doi:10.20944/preprints202410.0769.v1

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 [37] presented NOKIA S60 software profiling tools that allow developers to assess 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. [19] 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. The multimeter was assigned to measure the voltage across a resistor at a frequency of 10,000 hertz. The power value was determined by multiplying the resultant voltage with the input voltage and dividing by the resistance, as specified in formula (4). The energy consumption for each encryption and decryption task was calculated using formula (5), where 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 [38]. This system, which combines a main PC, NetDAQ, 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 assess the proposed LWBC for IoT devices comprehensively. 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.

5. 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.

 doi:10.20944/preprints202410.0769.v1

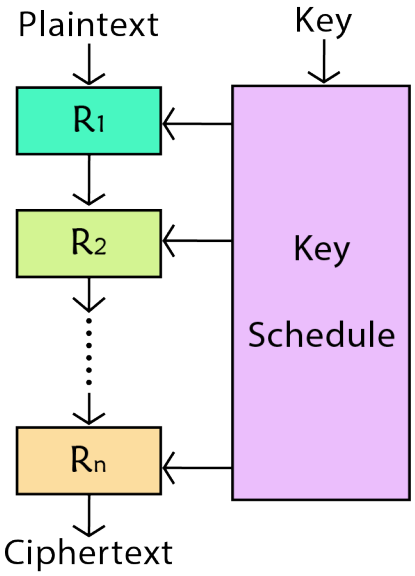

Figure 1. General architecture of LWBC showing rounds.

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.

 doi:10.20944/preprints202410.0769.v1

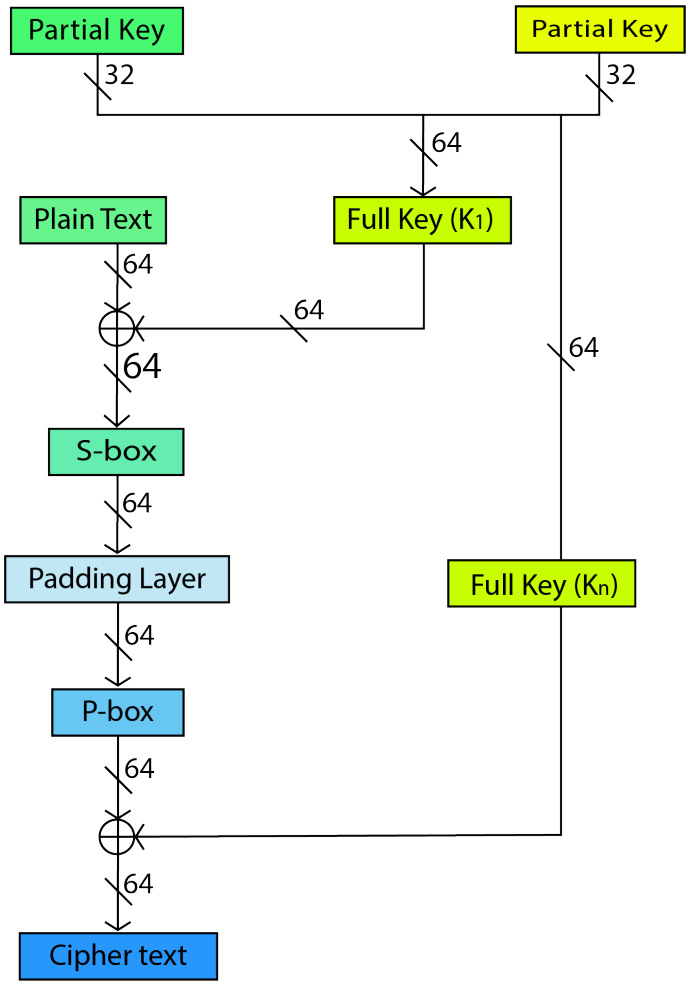

Figure 2. Diagram of the proposed LWBC.

5.1. Key Management

The utilisation of 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 inputting 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[6]. 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 minimise 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.

 doi:10.20944/preprints202410.0769.v1

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 who might possess 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.

5.2. 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 [39]. 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 [40].

5.3. 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.

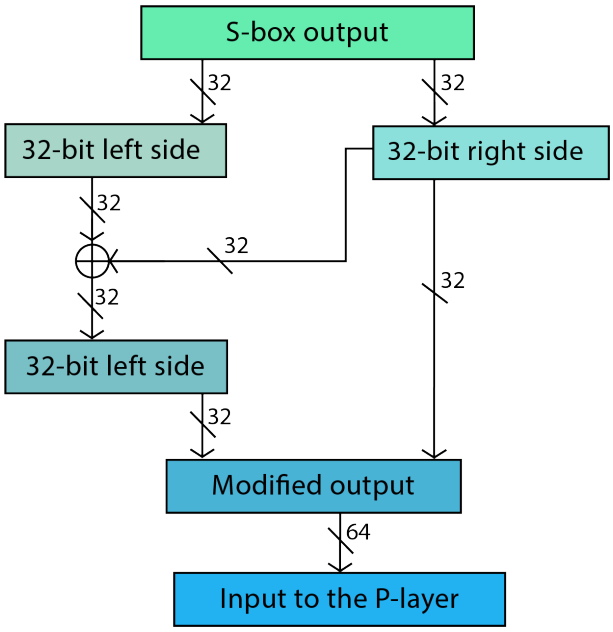

Figure 3. Middle layer of the proposed cipher.

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

 doi:10.20944/preprints202410.0769.v1

S-box output. The enhanced data is subsequently transmitted to the P-layer. Our SPN-based cipher offers comparable security to 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.

5.4. 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 1 is an example of the 64-bit P-box generated by 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 for 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.

 doi:10.20944/preprints202410.0769.v1


```
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.

Table 1. 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

 doi:10.20944/preprints202410.0769.v1

6. 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 algorithms on different platforms. By highlighting the power consumption of security processes on Arduino, we demonstrate the versatility and possible applicability of our architecture in various scenarios. Our specialised study setup is flexible and enables us to analyse the execution of different security applications on multiple systems.

The Arduino NodeMCU V3 is the selected platform for analysing the energy usage of the LWBC algorithm, as shown in Figure 5 [41]. This widely used development board is equipped with a high-performance Tensilica Xtensa® 32-bit RISC processor running at 80MHz, which offers sufficient processing capability for executing algorithms. Equipped with 4 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 the LWBC analysis [42].

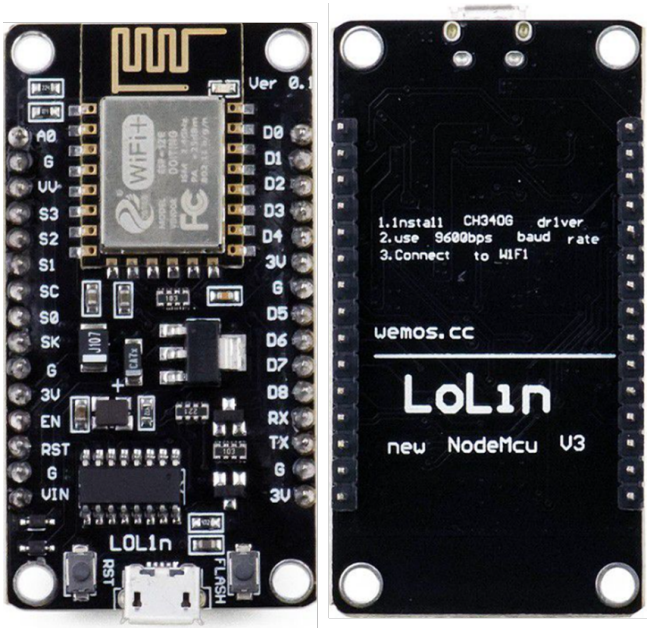

Figure 5. Arduino ESP8266 NodeMCU V3 device front and back view.

Our methodology involves doing all measurements outside of the component, ensuring that our approach remains independent of the device's individual properties. The inherent lightweight nature of this architectural style allows for versatile measurement capabilities across a range of 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 Figure 6.

 doi:10.20944/preprints202410.0769.v1

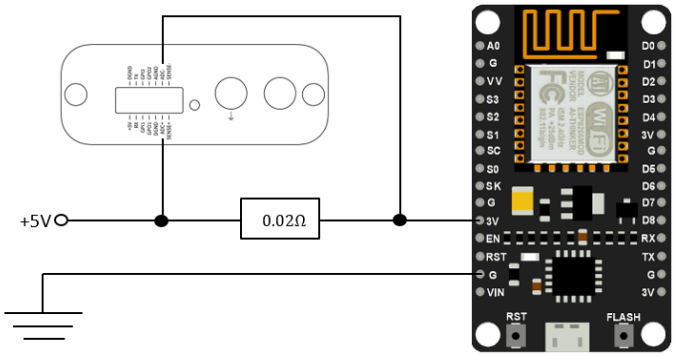

Figure 6. Schematic diagram of a USB power line, featuring a shunt resistor and an ADC.

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 adequately low is essential to minimise the voltage drop at the input of the device while guaranteeing that our sensor can detect the drop. In our measurements, we employ the minimum resistance value that our sensor can precisely detect, opting for a shunt resistor with a resistance of 0.02Ω and ADC measurement point.

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

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

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 made 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 a lot of different 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) allows precise monitoring of fast current fluctuations, making it well-suited for high-frequency situations. The Otii Arc is equipped with user-friendly software that is 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 [43].

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 7 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 equation.

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

 doi:10.20944/preprints202410.0769.v1

Figure 7. Qoitech Otii Arc power measuring device.

The experimental structure utilises the Otii Arc 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 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.

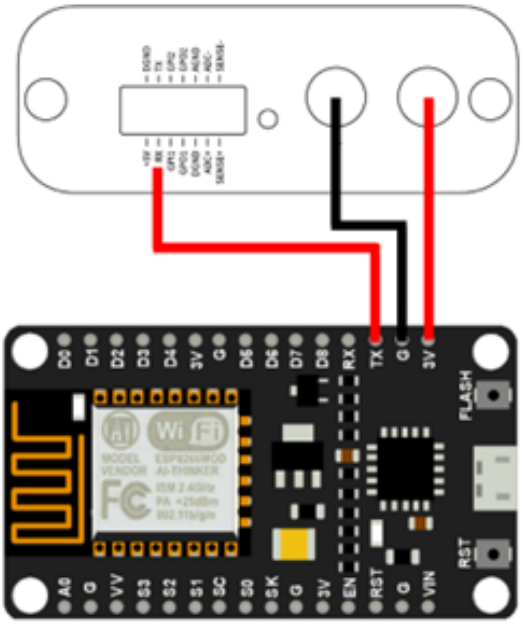

Figure 8. Connection diagram between Otii and IoT device.

The existing methodology offers a meticulous approach to assessing 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.

7. Experimental Results and Discussions

The following sections of this research will provide a comprehensive evaluation of the suggested LWBC,

 doi:10.20944/preprints202410.0769.v1

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 2 presents a comparison between 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 in relation to current algorithms. Important 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 100MHz), 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 analyse 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, with a focus on resource allocation, specifically power consumption, followed by security analysis.

Table 2. 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 (@100MHz Kbps/KB)
Proposed Cipher	Partial Key or half key	64	10	SPN	4.50	1450	1408	11,892	180
Piccolo [44]	Full key	64	25, 30	GFN	4.80	1136	2654	25,681	237
RECTANGLE [21]	Full key	64	25	SPN	5.96	1787	-	-	246
PRINT [24]	Full key	48	48	SPN	7.54	503	6210	35,161	100
PRESENT [22]	Full key	64	31	SPN	11.77	1570	1562	10,792	200
PUFFIN [45]	Full key	64	32	SPN	19.32	2577	-	1,240	200
ICEBERG [46, 47]	Full key	64	16	SPN	21.81	5800	-	16,660	400
HIGH [26]	Full key	64	32	ARX+GFN	29.14	3048	1340	-	470
TEA [11, 47,48]	Full key	64	64	Fiestel	35.32	3872	1354	9,129	194

7.1. Resource Utilisation Analysis

The practical implementation of cryptographic solutions in the context of the IoT is subject to the efficient utilisation of resources, particularly concerning power consumption. This section of

 doi:10.20944/preprints202410.0769.v1

the analysis is intended to evaluate the proposed cipher's power efficiency comprehensively. 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 [49].

7.1.1. Energy Consumption Analysis

This analysis aims to measure and understand the power and current demands of a lightweight block 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 utilised 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 six.

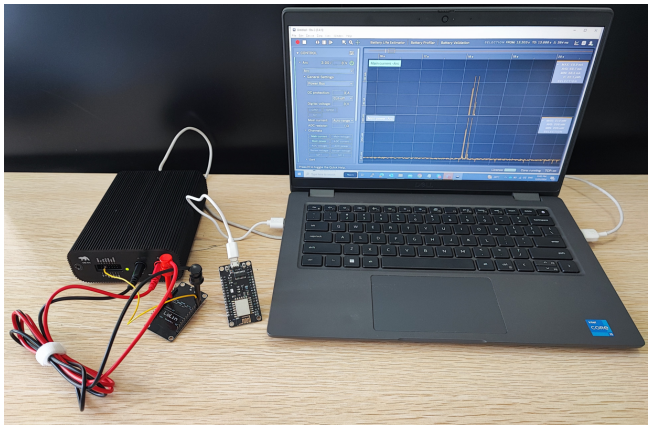

Figure 9. A physical connection between devices while measuring power consumption.

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, which involves transforming a 64-bit plaintext to ciphertext and vice versa, is completed in 2.1 milliseconds (equal to 2.1 x 10-3 seconds). By multiplying the values of power and time, we can determine the overall energy usage, which amounts to 290 microjoules.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 October 2024 doi:10.20944/preprints202410.0769.v1

Figure 10. Power consumption measurement by Otii Arc.

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. This quantitatively measures the performance of the cipher 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.

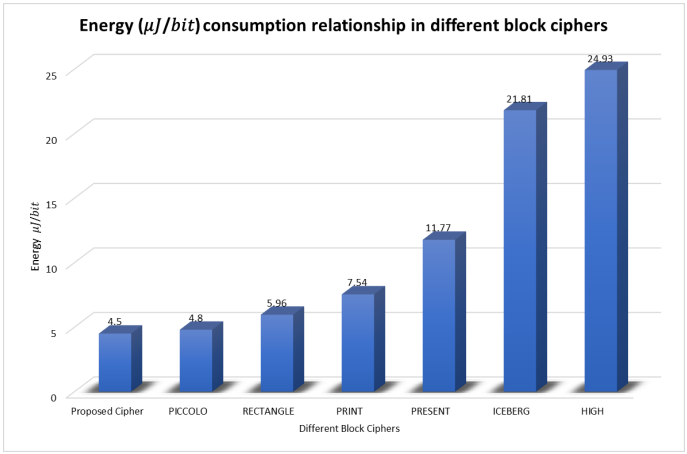

Figure 11. Evaluate various LWBCs' energy consumption.

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

 doi:10.20944/preprints202410.0769.v1

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.

7.1.2. 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 is 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.

7.1.3. 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 aspect 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 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.

7.1.4. 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. Using a multi-tiered security system enhances intricacy and resilience, protecting against prevalent threats, particularly in IoT devices with limited resources.

 doi:10.20944/preprints202410.0769.v1

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.

7.1.5. 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 the sake of 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.

7.1.6. Bate Area (GE)

The gate area (GE) is a key parameter to evaluate 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 [50].

The proposed cipher for the LWBC gate area is strategically designed to provide a footprint of 1450 GE that offers a balance between compactness and functionality that surpasses several existing ciphers such as RECTANGLE, PRESENT, PUFFIN, ICEBERG, HIGH, and TEA. This balance between compactness and functionality 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 is 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 minimising 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

 doi:10.20944/preprints202410.0769.v1

advantage make it a strong contender in the field and supports its potential for broader implementation in IoT environments.

7.1.7. 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). 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 very low 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.

7.1.8. Latency

Table 2 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 in comparison to PRESENT (10,792 cycles/block), and TEA (9,129 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.

7.1.9. 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.

 doi:10.20944/preprints202410.0769.v1

7.2. 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 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.

7.2.1. 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. The time needed to launch a brute force attack on a 64-bit cipher must be improved with current technology. Hence, it is essential to have a robust and secure encryption mechanism in place to safeguard against potential attacks.

7.2.2. Man-in-the-Middle Attack

A MitM attack is a cyber-attack 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

 doi:10.20944/preprints202410.0769.v1

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.

7.2.3. Side-Channel Attack

The LWBC we have developed demonstrates improved resistance to side-channel attacks, which are especially significant in cryptography for IoT devices. Side-channel attacks leverage data disclosed by the physical execution of a cryptosystem, including factors like time, power usage, and electromagnetic radiation. Nevertheless, the proposed cipher effectively mitigates these attacks by incorporating multiple resilient characteristics. A noteworthy feature is producing a fresh 64-bit key for every encryption cycle derived from a pool of 32-bit keys. This greatly enhances the level of unpredictability. The inherent unpredictability of this randomisation process, mainly when the keys are selected from diverse devices in an order list, is a significant obstacle for potential attackers attempting to anticipate or infer key details from side-channel data.

Furthermore, the cipher's structure includes a robust S-box and P-box to create confusion and diffusion, coupled with iterative processing that involves XOR operations and data chunking. Combining these elements introduces multiple difficulty levels, impeding the direct examination of side-channel leaks. The iterative nature of the cipher, characterised by many changes and modifications throughout each encryption phase, modifies the identifiable side-channel signatures. This makes it more challenging for attackers to establish a correlation between specific encryption stages and the observed data. Although it is impossible to achieve complete immunity to side-channel assaults, the design concepts and operating processes of our LWBC greatly enhance its protection against these weaknesses.

7.3. 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 μ J/bit. The low energy need of this technology is a crucial advantage in IoT situations

8. Conclusions

The comprehensive investigation into the proposed
LWBC has unveiled a compelling cryptographic solution tailored specifically for the complex realm of IoT applications. The focal point of our study has been a meticulous analysis of the LWBC's power consumption and overall efficiency, supplemented by an in-depth exploration of its security features through rigorous security analysis.

A standout feature of the proposed LWBC lies in its extraordinary power efficiency, boasting a minimal consumption rate of 4.5 microjoules per bit. This efficiency not only prolongs the lifespan of

 doi:10.20944/preprints202410.0769.v1

IoT device batteries but also positions the cipher as an ideal candidate for energy-sensitive scenarios, such as in energy-harvesting or low-power environments. The cipher's innovative design, which includes a 64-bit key, a single-round architecture with dynamic key updates, and resilience against common cryptographic attacks, underscores its commitment to robust security measures.

The security analysis component further strengthens the LWBC's credibility. The cipher's resistance to brute force attacks is fortified by its vast 64-bit key space, making decryption through exhaustive key search a formidable challenge. The LWBC demonstrates its resilience against MitM attacks, as even minor alterations to the ciphertext result in unintelligible deciphered data, ensuring the integrity and confidentiality of the information. Additionally, the LWBC exhibits heightened resistance to side-channel attacks, leveraging dynamic key generation and a sophisticated S-box and P-box architecture to mitigate vulnerabilities associated with physical data execution.

The proposed LWBC's versatility is emphasised by its balanced approach across key dimensions, including key and block size, rounds, cipher architecture, gate area, ROM, latency, and throughput. Its compact gate area of 1450 GE and a tiny ROM size of 1408 bytes contribute to its efficiency in terms of hardware footprint, which is vital for IoT applications with limited resources. Its performance in latency and throughput positions the cipher as a competitive solution in real-world IoT scenarios.

In essence, the proposed LWBC excels in power efficiency and security and showcases adaptability to the dynamic landscape of IoT. Its intrinsic ability to balance security and efficiency makes it a compelling choice for safeguarding sensitive data in the challenging and resource-constrained environments characteristic of IoT applications. The cipher's holistic strengths, encompassing power optimisation, security robustness, and efficient resource utilisation, mark it as a pioneering development in lightweight cryptography, poised to make significant contributions to the evolving field of IoT security.

References

1. Atlam, H.F., Alenezi, A., Alharthi, A., Walters, R.J. and Wills, G.B., 2017, June. Integration of cloud computing with internet of things: challenges and open issues. In 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) (pp. 670-675). IEEE.
2. Atlam, H.F., Alenezi, A., Alharthi, A., Walters, R.J. and Wills, G.B., 2017, June. Integration of cloud computing with internet of things: challenges and open issues. In 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) (pp. 670-675). IEEE.
3. Rana, M., Mamun, Q. and Islam, R., 2023. A block cipher for resource-constrained IoT devices. World Academy of Science, Engineering and Technology, 17(3), pp.266-271.
4. Rana, M., Mamun, Q. and Islam, R., 2021. An S-box design using irreducible polynomial with affine transformation for lightweight cipher. In Quality, Reliability, Security and Robustness in Heterogeneous Systems: 17th EAI International Conference, QShine 2021, Virtual Event, November 29–30, 2021, Proceedings 17 (pp. 214-227). Springer International Publishing.
5. Rana, M., Mamun, Q. and Islam, R., 2024, April. P-Box Design in Lightweight Block Ciphers: Leveraging Nonlinear Feedback Shift Registers. In 2024 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1-8). IEEE.
6. Rana, M., Mamun, Q. and Islam, R., 2023. Enhancing IoT security: an innovative key management system for lightweight block ciphers. Sensors, 23(18), p.7678.
7. Caforio, A., Balli, F., Banik, S. and Regazzoni, F., 2021, February. A deeper look at the energy consumption of lightweight block ciphers. In 2021 Design, Automation & Test in Europe Conference & Exhibition (DATE) (pp. 170-175). IEEE.
8. Zitouni, N., Sedrati, M. and Behaz, A., 2024. LightWeight energy-efficient Block Cipher based on DNA cryptography to secure data in internet of medical things devices. International Journal of Information Technology, 16(2), pp.967-977.

9. Fan, R., Cui, Y., Chen, Q., Wang, M., Zhang, Y., Zheng, W. and Li, Z., 2023, October. 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 (pp. 411-423).
10. Yang, K., Shi, Y. and Ding, Z., 2019. Data shuffling in wireless distributed computing via low-rank optimization. IEEE transactions on signal processing, 67(12), pp.3087-3099.
11. Cazorla, M., Marquet, K. and Minier, M., 2013, July. Survey and benchmark of lightweight block ciphers for wireless sensor networks. In 2013 international conference on security and cryptography (SECRYPT) (pp. 1-6). IEEE.
12. Mohd, B.J. and Hayajneh, T., 2018. Lightweight block ciphers for IoT: Energy optimization and survivability techniques. IEEE Access, 6, pp.35966-35978.
13. Mishra, R., Okade, M. and Mahapatra, K., 2022, September. FPGA based High Throughput Substitution Box Architectures for Lightweight Block Ciphers. In 2022 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA) (pp. 1-7). IEEE.
14. Fan, T., Li, L., Wei, Y. and Pasalic, E., 2022. Differential cryptanalysis of full-round ANU-II ultra-lightweight block cipher. International Journal of Distributed Sensor Networks, 18(9), p.15501329221119398.
15. Mhaouch, A., Elhamzi, W., Abdelali, A.B. and Atri, M., 2022. Optimized piccolo lightweight block cipher: Area efficient implementation. Traitement du Signal, 39(3), p.805.
16. Nadeem, A. and Javed, M.Y., 2005, August. A performance comparison of data encryption algorithms. In 2005 international Conference on information and communication technologies (pp. 84-89). IEEE.
17. Prasithsangaree, P. and Krishnamurthy, P., 2003, December. Analysis of energy consumption of RC4 and AES algorithms in wireless LANs. In GLOBECOM'03. IEEE Global Telecommunications Conference (IEEE Cat. No. 03CH37489) (Vol. 3, pp. 1445-1449). IEEE.
18. Grossschadl, J., Tillich, S., Rechberger, C., Hofmann, M. and Medwed, M., 2007, April. Energy evaluation of software implementations of block ciphers under memory constraints. In 2007 Design, Automation & Test in Europe Conference & Exhibition (pp. 1-6). IEEE.
19. Hager, C.T., Midkiff, S.F., Park, J.M. and Martin, T.L., 2005, March. Performance and energy efficiency of block ciphers in personal digital assistants. In Third IEEE International Conference on Pervasive Computing and Communications (pp. 127-136). IEEE.
20. Rana, M., Mamun, Q. and Islam, R., 2023. A block cipher for resource-constrained IoT devices. World Academy of Science, Engineering and Technology, 17(3), pp.266-271.
21. Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B. and Verbauwhede, I., 2014. RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms. Cryptology ePrint Archive.
22. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J., Seurin, Y. and Vikkelsoe, C., 2007. PRESENT: An ultra-lightweight block cipher. In Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9 (pp. 450-466). Springer Berlin Heidelberg.
23. Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T. and Shirai, T., 2011. Piccolo: an ultra-lightweight blockcipher. In Cryptographic Hardware and Embedded Systems–CHES 2011: 13th International Workshop, Nara, Japan, September 28–October 1, 2011. Proceedings 13 (pp. 342-357). Springer Berlin Heidelberg.
24. Knudsen, L., Leander, G., Poschmann, A. and Robshaw, M.J., 2010. PRINTcipher: a block cipher for IC-printing. In Cryptographic Hardware and Embedded Systems, CHES 2010: 12th International Workshop, Santa Barbara, USA, August 17-20, 2010. Proceedings 12 (pp. 16-32). Springer Berlin Heidelberg.
25. Sun, Y., Wang, M., Jiang, S. and Sun, Q., 2012. Differential cryptanalysis of reduced-round ICEBERG. In Progress in Cryptology-AFRICACRYPT 2012: 5th International Conference on Cryptology in Africa, Ifrance, Morocco, July 10-12, 2012. Proceedings 5 (pp. 155-171). Springer Berlin Heidelberg.
26. Hong, D., Sung, J., Hong, S., Lim, J., Lee, S., Koo, B.S., Lee, C., Chang, D., Lee, J., Jeong, K. and Kim, H., 2006. HIGHT: A new block cipher suitable for low-resource device. In Cryptographic Hardware and Embedded Systems-CHES 2006: 8th International Workshop, Yokohama, Japan, October 10-13, 2006. Proceedings 8 (pp. 46-59). Springer Berlin Heidelberg.
27. Rivest, R.L., 1994, December. The RC5 encryption algorithm. In International Workshop on Fast Software Encryption (pp. 86-96). Berlin, Heidelberg: Springer Berlin Heidelberg.

28. Ye, W., Vijaykrishnan, N., Kandemir, M. and Irwin, M.J., 2000, June. The design and use of simplepower: a cycle-accurate energy estimation tool. In Proceedings of the 37th Annual Design Automation Conference (pp. 340-345).
29. Brooks, D., Tiwari, V. and Martonosi, M., 2000. Wattch: A framework for architectural-level power analysis and optimizations. ACM SIGARCH Computer Architecture News, 28(2), pp.83-94.
30. Sinha, A. and Chandrakasan, A.P., 2001, June. Jouletrack: A web based tool for software energy profiling. In Proceedings of the 38th annual design automation conference (pp. 220-225).
31. Austin, T., Larson, E. and Ernst, D., 2002. SimpleScalar: An infrastructure for computer system modeling. Computer, 35(2), pp.59-67.
32. Pathak, A., Hu, Y.C. and Zhang, M., 2012, April. 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 (pp. 29-42).
33. Huang, J., Qian, F., Gerber, A., Mao, Z.M., Sen, S. and Spatscheck, O., 2012, June. A close examination of performance and power characteristics of 4G LTE networks. In Proceedings of the 10th international conference on Mobile systems, applications, and services (pp. 225-238).
34. Zhang, L., Tiwana, B., Qian, Z., Wang, Z., Dick, R.P., Mao, Z.M. and Yang, L., 2010, October. 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 (pp. 105-114).
35. Carroll, A. and Heiser, G., 2010. An analysis of power consumption in a smartphone. In 2010 USENIX Annual Technical Conference (USENIX ATC 10).
36. Fitzek, F.H. and Reichert, F. eds., 2007. Mobile Phone Programming: and its Application to Wireless Networking. Springer Science & Business Media.
37. Creus, G.B. and Kuulusa, M., 2007. Optimizing mobile software with built-in power profiling. In Mobile Phone Programming: Application to Wireless Networking (pp. 449-462). Dordrecht: Springer Netherlands.
38. Nie, T., Zhou, L. and Lu, Z.M., 2014. Power evaluation methods for data encryption algorithms. IET software, 8(1), pp.12-18.
39. Razaq, A., Alhamzi, G., Abbas, S., Ahmad, M. and Razzaque, A., 2023. Secure communication through reliable S-box design: A proposed approach using coset graphs and matrix operations. Heliyon, 9(5).
40. Rana, M., Mamun, Q. and Islam, R., 2021. An S-box design using irreducible polynomial with affine transformation for lightweight cipher. In Quality, Reliability, Security and Robustness in Heterogeneous Systems: 17th EAI International Conference, QShine 2021, Virtual Event, November 29–30, 2021, Proceedings 17 (pp. 214-227). Springer International Publishing.
41. Kashyap, M., Sharma, V. and Gupta, N., 2018. Taking MQTT and NodeMcu to IOT: communication in Internet of Things. Procedia computer science, 132, pp.1611-1618.
42. Arduino. "arduino esp8266 nodemcu v3 " Arduino. https://www.arduino.cc/ (accessed 02/02/2024, 2024).
43. Q. AB. "Extend battery life. Deliver quality." https://www.qoitech.com/ (accessed 02/02/2024, 2024).
44. Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T. and Shirai, T., 2011. Piccolo: an ultra-lightweight blockcipher. In Cryptographic Hardware and Embedded Systems–CHES 2011: 13th International Workshop, Nara, Japan, September 28–October 1, 2011. Proceedings 13 (pp. 342-357). Springer Berlin Heidelberg.
45. Cheng, H., Heys, H.M. and Wang, C., 2008, September. Puffin: A novel compact block cipher targeted to embedded digital systems. In 2008 11th EUROMICRO Conference on Digital System Design Architectures, Methods and Tools (pp. 383-390). IEEE.
46. Cheng, H. and Heys, H.M., 2008, May. Compact ASIC implementation of the ICEBERG block cipher with concurrent error detection. In 2008 IEEE International Symposium on Circuits and Systems (ISCAS) (pp. 2921-2924). IEEE.
47. S. Ragupathy, and T, Mythili,"Energy optimized simon lightweight security algorithm for internet of medical things (IoMT)," International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 8.
48. Mishra, Z. and Acharya, B., 2021. High throughput novel architectures of TEA family for high speed IoT and RFID applications. Journal of Information Security and Applications, 61, p.102906.
49. Eisenbarth, T., Kumar, S., Paar, C., Poschmann, A. and Uhsadel, L., 2007. A survey of lightweight-cryptography implementations. IEEE Design & Test of Computers, 24(6), pp.522-533.

 doi:10.20944/preprints202410.0769.v1

50. Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I. and Manifavas, C., 2018. A review of lightweight block ciphers. Journal of cryptographic Engineering, 8, pp.141-184.