Comprehensive Survey of Lightweight Ciphers for Resource-Constrained IoT Devices

Eyas A. Al-Yousfi [1,*]
Mohammed Alkhawlani [1]

[1] Department of Electronics Engineering, Faculty of Engineering, University of Science and Technology, Sana'a, Yemen

* Corresponding authors: eyasalyousfi@gmail.com

https://doi.org/10.59222/ustjet.3.1.4

Comprehensive Survey of Lightweight Ciphers for Resource-Constrained IoT Devices

Abstract:

The rapid growth of IoT devices has highlighted the need for effective security solutions suitable for resource-constrained environments. Since traditional cryptography methods are often computationally expensive, this has resulted in the creation of lightweight cryptography (LWC), which aims to develop efficient ciphers that balance security, performance, and resource efficiency. This survey paper explores lightweight cryptographic algorithms, mainly hardware-based block ciphers, by analyzing 43 widely used ciphers based on key metrics in hardware implementation such as throughput, efficiency, energy consumption, and hardware area. These metrics are critical for evaluating cryptographic solutions for IoT devices with constrained resources. The study identifies trade-offs between security, performance, and resource efficiency, with some ciphers performing well in high-speed applications and others optimized for low energy and minimal hardware use. By providing a comparative analysis, this work aims to assist researchers and developers in selecting suitable cryptographic solutions, contributing to the advancement of IoT security and encouraging further exploration in this important area.

Keywords: Cryptography, lightweight cryptography (LWC), Internet of Things (IoT), block Ciphers, hardware implementation.

https://doi.org/10.59222/ustjet.3.1.4

دراسة شاملة للتشفير خفيف الوزن لأجهزة إنترنت الأشياء محدودة الموارد

الملخص:

أبرز النمو السريع لأجهزة إنترنت الأشياء الحاجة إلى حلول أمنية فعّالة مناسبة للبيئات ذات الموارد المحدودة. ونظرًا لأن طرق التشفير التقليدية غالبًا ما تكون مكلفة من الناحية الحسابية، فقد أدى ذلك إلى إنشاء التشفير خفيف الوزن (LWC)، الذي يهدف إلى تطوير شفرات فعالة توازن بين الأمان، الأداء، وكفاءة الموارد. تستكشف هذه الدراسة خوارزميات التشفير الخفيفة، وخاصة التشفير الكتلي القائم على الأجهزة، من خلال تحليل 43 شفرة مستخدمة على نطاق واسع استنادًا إلى مقاييس رئيسية في تنفيذ الأجهزة مثل الإنتاجية والكفاءة واستهلاك الطاقة ومساحة الأجهزة. تعد هذه المقاييس بالغة الأهمية لتقييم الحلول التشفيرية لأجهزة إنترنت الأشياء ذات الموارد المحدودة. تكشف الدراسة عن المقايضات بين الأمان، الأداء، وكفاءة الموارد، حيث أظهرت بعض الخوارزميات أداءً ممتازًا في التطبيقات التي تتطلب سرعة عالية، بينما تم تحسين أخرى لتكون مناسبة للتطبيقات ذات استهلاك الطاقة المنخفض واستخدام العتاد المحدود. من خلال تقديم تحليل مقارن، تهدف هذه الدراسة إلى مساعدة الباحثين والمطورين في اختيار حلول تشفير مناسبة، مما يسهم في تطوير أمن إنترنت الأشياء ويشجع على مزيد من الاستكشاف في هذا المجال المهم.

الكلمات المفتاحية: التشفير، التشفير خفيف الوزن (LWC)، إنترنت الأشياء (IoT)، التشفير الكتلي، التنفيذ المادي.

1. Introduction

In recent years, the Internet of Things (IoT) becomes one of the hottest research areas. IoT has appeared as a novel technology that can change our future and life. IoT promises better safety, enhances management of patients, improves energy efficiency, reports the changes in environment, prevents fires, optimizes manufacturing processes, and offers many more beneficial functionality [1-6].

IoT is defined by several definitions, one of the most common and widely acceptable definition is that IoT is a technology that allows people and things to be connected anytime, anyplace, with anything and anyone, ideally using any path/network and any service [7]. A second definition that has been introduced by the Cisco Internet Business Solutions Group (IBSG) stated that IoT is simply the point in time when more things or objects were connected to the Internet than people [8, 9].

Despite the great promise and benefits of the Internet of Things (IoT), there are many challenges in its environment that affect how well this technology works [1-4].

Internet of Things technology faces many challenges. Security is one of the main challenges for IoT technology. Without providing appropriate security, some attackers might want to control some devices directly or indirectly, and this massive technology will be misused. Because IoT will create a need to manage large numbers of different types of devices, it will be more susceptible to being attacked than the Internet [1, 6, 10-18].

The massive quantity and diversity of these devices will increase the potential attack surface. Gartner estimates that by 2020, more than 25 percent of all enterprise attackers will make use of the IoT [19].

The challenge of preventing attacks will be compounded by IoT deployments where technical expertise is absent, such as homes and small enterprises [12].

Recently a study by HP reveals that 70% of the devices in IoT are vulnerable to attacks [20], and a global customer survey shows that security and privacy are the main IoT concern [21].

https://doi.org/10.59222/ustjet.3.1.4

Professionals with extensive resources and a high level of technical knowledge increasingly carry out hacking attacks, and since the IoT affects people's daily lives and industrial operations, there will be plenty of incentives to hack IoT systems. Especially, many current IoT devices are very easy to hack [22].

From an operational technology perspective, the Industrial IoT (IIoT) makes industrial control systems more autonomous and connected [23]. Hence a successful attack on an IIoT system has the potential to be as serious as the worst industrial accidents [24]. Therefore, it is critical to secure this emerging technology revolution [2].

Upon analyzing the structure of the Internet of Things (IoT) system, it is apparent that IoT end devices represent the most critical vulnerability. Conventional cryptography technologies and methodologies are often computationally expensive, and the deployment of such algorithms tends to hinder the performance of resource-constrained devices typically employed in IoT applications. Consequently, a balance must be struck to achieve the dual objectives of ensuring robust security while maintaining minimal computational overhead. This challenge has given rise to the field of lightweight cryptography (LWC), which focuses on developing novel algorithms specifically designed to address this issue [25, 26].

This survey paper is organized as follows: Section 2 introduces the concept of lightweight cryptography (LWC) and provides a general classification of LWC algorithms. Section 3 reviews the most significant lightweight block encryption algorithms studied in previous research, along with the performance evaluation criteria for LWC. Section 4 presents a comparative analysis and discussion of the previous research results. Finally, Section 6 presents the conclusions and key remarks.

2. Lightweight Cryptography (LWC)

LWC is a junction of two terms "Light and weight", and it is a sector of a classical cryptographic algorithm. LWC is generally defined as cryptography for resource-constrained devices [25].

Implementing a lightweight cipher in either software or hardware is a challenging task that requires achieving an optimal trade-off between security and performance metrics. Hardware implementations are generally preferred for their ability to deliver faster processing speeds and lower power and energy consumption compared to their software counterparts. Among

the available hardware implementation approaches, Application-Specific Integrated Circuits (ASICs) and Field-Programmable Gate Arrays (FPGAs) are widely utilized. While ASICs have traditionally been faster than FPGAs, advancements in process technologies have significantly narrowed the performance gap between the two [27]. Furthermore, FPGAs offer a cost-effective and highly flexible development platform. Their inherent advantages, such as algorithm agility, ease of updates and modifications, architectural efficiency, and optimized resource utilization, make them particularly well-suited for cipher implementations [28].

LWC algorithms are mainly divided into two major categories of algorithms: symmetric ciphers and asymmetric ciphers. Types of symmetric ciphers include block and stream ciphers. Each part is discussed in more detail in the next sections. Figure 1 shows the main categories of LWC algorithms.

2.1 Asymmetric Cipher

Asymmetric cipher is conjointly referred to as public-key cryptography (PKC). PKC algorithms use a key pair, where one of the keys is private and the other public. The sender has the receiver's public key, whereas the private key is not known.

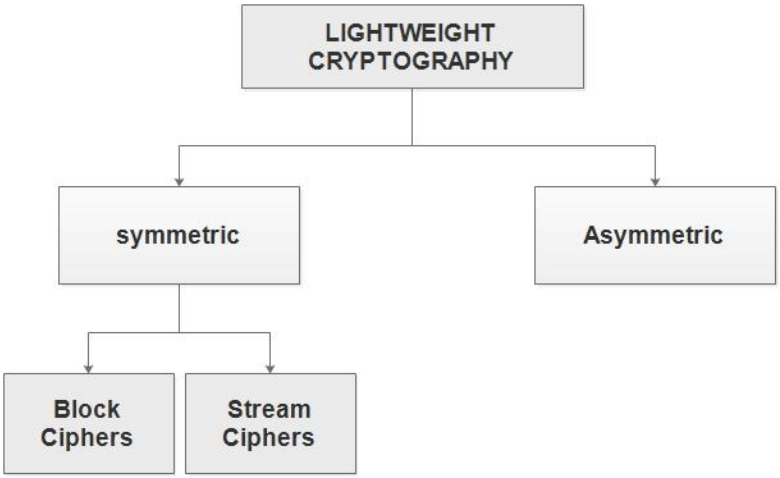

Figure 1: The Main Categories of LWC Algorithms

https://doi.org/10.59222/ustjet.3.1.4

The receiver ought to produce his try of the public and private key and publish his public key while not considering its security. The key pair is generally created from a mathematical function that establishes a relation between the private and the public key, but with special properties to avoid deriving the private key from the public one [29-32].

PKC is critical for networked environments. It has been used in encryption, digital signatures, and key establishment to provide confidentiality, integrity, authentication, nonrepudiation, availability, and access control services. [32]

Rivest–Shamir–Adleman (RSA) algorithm is one of the most popular and widely used asymmetric encryption algorithms. It was developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman and took its name from them.

Although RSA is the most popular and secure asymmetric encryption algorithm in terms of key difficulty, it takes a long time to encrypt and decrypt. Besides, a security flaw appears that encrypting the same message again produces the same encrypted message [31, 33].

Elliptic Curve Cryptography (ECC) is presently the most popular asymmetric option chosen to provide security in IoT systems due to its high security and small size. ECC uses the mathematics of elliptic curves. ECC is considered the next generation of RSA. The main difference between ECC and RSA is the strength of the key. A 160-bit key in ECC is equivalent in power to a 1024-bit key in RSA. Thus, ECC uses a smaller key size to achieve a similar security level compared to RSA.

ECC is characterized by the speed of obtaining the keys and less memory to store them. On the other hand, a challenge for ECC is that it cannot be implemented as efficiently as RSA [32, 34-36]. In recent years, the de nations for new elliptic curves not only seek to achieve high-security levels but also to reduce operational costs and to reduce the hardware resources required to perform computations efficiently [37-59].

Therefore, based on the preceding, Asymmetric ciphers use a larger key size and more memory consumption, which makes this cipher less popular in terms of IoT security these algorithms are not compatible with the discrepancy in the capabilities of IoT devices and therefore cannot be used in building security systems in term of encryption. Hence, we find that symmetric encryption is more suitable for such systems.

For example, AES is 100–1000 times quicker than ECC on 8-bit microcontrollers However; this does not detract from its value, as it cannot be dispensed with in verification, key exchange, and signature operations [60, 61].

2.2 Symmetric Cipher

In this encryption, the secret key is shared by each sender and receiver. As a result, it is utilized during the encryption and decryption processes. Block ciphers and stream ciphers are two types of symmetric ciphers. In this section, we›ll go into more detail about both types.

2.2.1 Stream Ciphers

Stream ciphers are symmetric ciphers that generate cipher text by encrypting plain text bit streams with associated key streams. Encryption on Stream Ciphers is all about the conversion of plain text performed by taking one byte of the plaintext at a time (at most 8 bits could get converted at a time), and for decryption XORing the encryption text will easily reverse the plaintext. Stream cipher also known as State Cipher, since encryption of each digit is dependent on the current state of the cipher [62, 63].

This type of encryption mainly uses the simplest possible operators. In most cases, an XOR operation is used between the plaintext bits and the corresponding key bits. Therefore, the throughput (encryption speed) of stream ciphers is much higher than block ciphers. They are also used in applications where the size of plaintext is unclear or continuous and in low-latency use cases.

But is considered less secure than block ciphers. Because every encrypted bit is independent of other bits (the data are encrypted bit by bit).

This type of encryption has been the subject of a lot of research in recent years [63-73], and researchers have developed algorithms that work well in IoT environments with constrained resources.

2.2.2 Block Ciphers

A block cipher is a symmetric cipher that processes an entire block of data at once. A block of n-bit data of a predetermined size is encrypted by the block cipher using encryption technology. Typically, a cipher block has a size of 64, 128, or 256 bits. Iterated block ciphers are used by most block cipher algorithms to transform fixed-size plaintext blocks into ciphertext blocks of the same size.

https://doi.org/10.59222/ustjet.3.1.4

In contrast to stream ciphers, block ciphers employ both confusion and diffusion principles, and their decryption is more complicated.

Block ciphers should have the most complex ciphertext and plaintext coherence possible. As stated by Claude Shannon in his 1949 publication, Theory of Secrecy Systems [74]. He clarified that a cipher must satisfy two crucial properties: diffusion and confusion. While Diffusion asserts that whenever one character in the plaintext changes, numerous characters in the ciphertext should likewise change, Confusion suggests that each character of the ciphertext should depend on multiple portions of the key [32, 62].

Based on their internal structure, the block ciphers can be categorized into two groups: Feistel networks (FN) and Substitution-permutation networks (SPN).

Other sources divide block ciphers into five categories, including SPNs, FNs, (NLFSR) Nonlinear-feedback shift register-based, hybrids, and (ARX) Add Rotate-XOR [27, 32, 62, 75].

SPN and Feistel structures are among the most widely used architectures in block ciphers. The Feistel structure employs the same circuit for both encryption and decryption, reducing implementation costs and ensuring low memory requirements [76]. However, despite these advantages, many Feistel-based ciphers face security challenges, making the Substitution-Permutation Network (SPN) a stronger contender in the field of lightweight cryptography. Unlike Feistel ciphers, SPN ciphers have demonstrated greater resilience against security vulnerabilities. As a result, SPN ciphers, particularly those designed exclusively for encryption, remain a highly competitive option and are often the preferred choice in the domain of lightweight cryptography (LWC) [77].

Because lightweight block ciphers have greater security than stream ciphers, many researchers in the field of lightweight encryption algorithms recommend them [62, 75, 78-102].

3. Comprehensive Review for LWC Related Work

Based on the above analysis, symmetric encryption algorithms are the most suitable choice for resource-constrained Internet of Things (IoT) environments, with block cipher algorithms being the preferred option. Among the various internal structures of block ciphers, the two most commonly used are Substitution-Permutation Networks (SPN) and Feistel Networks (FN).

Therefore, this section examines the most significant algorithms belonging to these two categories. As previously mentioned, these algorithms can be implemented in either software or hardware; however, we will focus on hardware-based implementations due to their advantages. Consequently, the algorithms under study will be classified into two groups: SPN and FN.

3.1 Substitution-Permutation Network (SPN)

NIST proposed AES in 2000, and it has since been considered a landmark with a significant impact on modern cryptography. thus, cannot be ignored in the context of LWC. The AES is sometimes referred to as the Rijndael. In the context of LWC, there is a lot of research related to AES. One of the most important research in hardware implementation [103]. The author of this research indicates that lightweight AES implementations require 2400 GE, which is about 23% less than the minimum for traditional AES implementations. Many studies [104-109] indicate that enhancing recognized and standard algorithms, like AES, is more effective than creating entirely new ones. This is especially true for AES, given its strong reputation, reliability, and proven security. By improving such trusted algorithms, we can benefit from their efficiency and reliability while adapting them for lightweight applications.

mCrypton (miniature of Crypton) [110] presents a new lightweight block cipher, specifically designed for resource-constrained devices such as low-cost RFID tags and sensors. mCrypton features a 64-bit block size and three key size options (64 bits, 96 bits, and 128 bits), focusing on efficiency in power consumption and resource usage. Its design is based on the Crypton [111] architecture, with simplifications and improvements to better suit the target applications. Experimental results demonstrate that mCrypton can be effectively implemented in hardware with a low gate count, making it suitable for economical devices.

The PRESENT cipher [112] was designed as an ultra-lightweight encryption algorithm optimized for hardware implementation. It operates on 64-bit data blocks with 80- or 128-bit keys and employs 31 rounds of iteration. In 2012, it was standardized by ISO/IEC. The cipher utilizes a single 4×4 S-box, performing 16 parallel S-box operations in the nonlinear substitution layer, along with bit permutations in the linear diffusion layer, effectively minimizing hardware resource consumption. PRESENT meets both lightweight and ultra-lightweight encryption requirements. It is among the first ciphers implemented on highly constrained devices.

https://doi.org/10.59222/ustjet.3.1.4

ICEBERG [113] is a high-speed involutive cipher designed for efficient encryption and decryption. It operates on 64-bit data blocks with 128-bit keys over 16 rounds. Optimized for reconfigurable hardware implementations, ICEBERG enables key changes at every clock cycle without any performance degradation, as it derives round keys on-the-fly. This design ensures highly efficient encryption/decryption processes while maintaining optimal resource utilization. With a hardware cost of 5800 gates, ICEBERG achieves a throughput of 400 Kbps.

PUFFIN-2 [114] is a lightweight cipher that operates on 64-bit blocks with an 80-bit key over 34 rounds. It is an improved version of its predecessor, PUFFIN (2303 GE) [92] , and is based on a serialized architecture that supports both encryption and decryption. In terms of hardware implementation, PUFFIN-2 achieves a significant reduction in physical area, occupying 1083 GE, which is approximately 16% smaller than the serialized implementation of PRESENT-80 (1296 GE).

PRINTcipher [115] is a lightweight encryption algorithm designed to meet the cryptographic needs of specific applications, such as Integrated Circuit (IC) printing and Electronic Product Code (EPC). It supports 80-bit and 160-bit keys with 48-bit and 96-bit blocks, respectively, operating over 48 and 96 rounds. PRINTcipher-48 (402 GE) is optimized for IC-printing applications, while PRINTcipher-96 (726 GE) is tailored for EPC encryption.

EPCBC [116] is a PRESENT-like cipher designed for EPC encryption, utilizing 96-bit keys with 48-bit or 96-bit block sizes over 32 rounds. Its primary contribution lies in adapting an improved version of PRESENT to support 96-bit keys, enhancing security for EPC applications. The design incorporates insights from the security analysis of PRESENT, implementing an optimized key scheduling procedure that strengthens resistance against related-key differential attacks.

Klein [96] is a lightweight cipher that operates on 64-bit blocks with key sizes of 64, 80, and 96 bits, requiring 12, 16, and 20 rounds, respectively. It employs a single 4-bit involutional S-box for nonlinear substitution, while its column mixing is inspired by the column transformation in AES, enhancing diffusion efficiency.

LED (Lightweight Encryption Device) is [117] a compact AES-like cipher designed to minimize hardware footprint while maintaining reasonable software performance. It supports 64-, 80-, 96-, and 128-bit keys with 64-bit

blocks, operating over 32 or 48 rounds. Unlike traditional ciphers, LED does not use a key scheduling process. Instead, it incorporates the PRESENT S-box, row-wise processing similar to lightweight AES [103], and the mix column approach from the PHOTON hash function [118], integrating modern trends in lightweight cryptographic design.

NOEKEON [119] is an early involutive cipher that operates on 128-bit keys and blocks over 16 identical rounds, enabling the reuse of the same circuitry for both encryption and decryption. Despite initial security concerns, its designers argued that the proposed attacks were impractical and that the cipher remained secure [120]. The first hardware implementation [121] occupies 2880 GE, making it suitable for lightweight devices.

PRINCE [122] is a low-latency cipher designed for efficient hardware implementation. It operates on 64-bit blocks with 128-bit keys over 12 rounds. Its lightweight design [123] requires 2953 GE, achieving a 533.3 Kbps throughput with low energy consumption. By reusing hardware for both encryption and decryption, PRINCE minimizes resource usage and further reduces latency.

I-PRESENT™ [124] is an involutive version of PRESENT, maintaining the same key and block sizes while operating over 30 rounds instead of 31. Inspired by PRINCE, its structure consists of a 15-round function followed by a 15-round involutive function. The S-box layer incorporates two additional 4×4 S-boxes, applied 16 times, while the NOEKEON S-box is used in the involutive function. The key schedule generates 30 round subkeys of 64 bits each, with decryption identical to encryption, except for the reverse order of subkey input. The most compact hardware implementation requires 2769 GE, supporting both encryption and decryption, whereas the encryption-only implementation of PRESENT requires 1570 GE.

RECTANGLE [125] is a lightweight SPN cipher designed for efficient implementation across various platforms. It operates on 64-bit blocks with 80- or 128-bit keys over 25 rounds. Utilizing a bit-slicing approach, it achieves ultra-lightweight performance. Its substitution layer consists of 16 parallel 4×4 S-boxes, balancing security and efficiency, while the permutation layer employs three rounds of circular shifts, effectively reducing hardware costs.

https://doi.org/10.59222/ustjet.3.1.4

PICO [126] is an ultra-lightweight cipher that operates on 64-bit blocks with 128-bit keys over 32 rounds. It features robust S-boxes and a well-designed permutation layer, ensuring a strong avalanche effect that enhances resistance against differential, linear, and other cryptographic attacks.

SKINNY [127] is an adjustable block cipher with flexible block, key, and tweak sizes, designed for low latency and strong security. In hardware implementations, it outperforms SIMON in terms of area efficiency and throughput, making it a highly optimized choice for lightweight encryption.

DULBC [128] is a dynamic lightweight cipher with a 64-bit block size, available in two variants: DULBC-80 and DULBC-128, depending on the key length, operating over 29 rounds. It features key-dependent round functions, providing a significant cryptanalysis complexity advantage over static ciphers.

IVLBC [129] is a lightweight cipher with a 64-bit block size and 80- or 128-bit key lengths, operating over 29 rounds. It utilizes lightweight involutional S-boxes and nibble-based permutations, enabling the reuse of circuits and code for both encryption and decryption. In hardware implementations, IVLBC-128 demonstrates a lower gate equivalent compared to PICO.

3.2 Feistel Network (FN)

The Data Encryption Standard (DES) is one of the earliest ciphers studied for lightweight cryptography (LWC). It operates on 64-bit blocks using a 56-bit key over 16 rounds. However, its primary drawback compared to AES is its smaller key size, which results in a lower security level. To address the circuit complexity of DES, the DESL variant was introduced, reusing a single S-box eight times to optimize hardware efficiency. While DESL maintained the same throughput as DES, it required approximately 20% less hardware area, occupying 1848 GE compared to 2309 GE for DES [130]. Another variant, DESX, enhances security by incorporating key whitening, which mitigates brute-force attacks. DESX retains the same block size and number of rounds as DES but uses a 184-bit key for improved security. Hardware implementations of DES and DESX are discussed in [130], with their respective hardware costs being 2309 GE and 2629 GE.

Camellia [131], developed by Nippon Telegraph and Telephone Corporation and Mitsubishi Electric Corporation, is a widely recognized block cipher approved by ISO/IEC, IETF, the NESSIE and CRYPTREC projects, and

included in Japan›s new e-Government Recommended Ciphers List. It gained popularity due to its comparable security level and processing efficiency with AES. Camellia employs the same block and key sizes as AES, operating through either 18 or 24 rounds. In the context of lightweight cryptography (LWC), it has been primarily analyzed for its fast software implementations, as its hardware implementation [132] exceeds the 3000GE threshold, requiring approximately 6511GE.

CLEFIA [133] is a lightweight block cipher developed by SONY and standardized under ISO/IEC 29192. It operates on 128-bit blocks with 128-, 192-, and 256-bit key options, requiring 18, 22, and 26 rounds, respectively. Known for its highly efficient hardware and software implementations, CLEFIA›s most compact encryption-only implementation [134] requires 2488 GE for a 128-bit key, while the encryption/decryption version occupies 2604 GE, making it 23% smaller than the equivalent AES-128 implementation. CLEFIA employs a serialized architecture that eliminates the need for additional registers, and decryption can be implemented with only a 116 GE overhead. To optimize performance, the designers utilized clock gating techniques to reduce the number of multiplexers while increasing cycle efficiency. Additionally, they incorporated techniques from compact AES implementations, such as column-wise computation in the matrix multiplier and the replacement of D flip-flops and multiplexers with scan flip-flops to further minimize area usage.

The Tiny Encryption Algorithm (TEA) [135, 136] is a lightweight cipher that operates on 64-bit blocks with 128-bit keys over 64 rounds, requiring 2355 GE for implementation. It is recognized for its efficiency in terms of power, energy, and memory usage, as well as its simplicity and ease of implementation. However, TEA has notable weaknesses, including vulnerability to equivalent key attacks and poor performance as a hash function. To address these issues, the eXtended TEA (XTEA) [137], also known as Block TEA, was introduced. While both ciphers were initially designed for software implementations, hardware implementations of XTEA have been reported [137], requiring 3490 GE, which exceeds the typical 3000 GE limit for lightweight cryptographic designs.

MIBS [138] is a lightweight block cipher that supports 64-bit blocks with 64- and 80-bit key options, operating over 32 rounds. It follows a Feistel structure with an SPN-based round function, incorporating the S-box from mCrypton.

https://doi.org/10.59222/ustjet.3.1.4

The round function of MIBS shares similarities with PRESENT, as both utilize the SPN structure and a single 4×4 S-box. In hardware implementations, MIBS-80 and PRESENT-80 exhibit comparable throughput and similar area occupancy, making MIBS a competitive choice for lightweight cryptographic applications.

In their effort to develop a lightweight variant of the Soviet GOST cipher, the authors in [139] achieved a hardware implementation requiring 651 gate equivalents (GEs). This implementation employs a 256-bit key and a 64-bit block size, structured as a Feistel network with 32 rounds. A significant contribution of this proposal is the adaptation of the PRESENT S-box, which effectively reduces the gate equivalent metric. The authors deliberately avoided employing straightforward wiring for permutation in order to minimize area, as this could compromise the cipher›s differential and linear cryptographic properties.

LBlock [101] is a lightweight block cipher featuring a 32-round structure with a 64-bit block size and an 80-bit key. Drawing inspiration from PRESENT, its key schedule employs a nonlinear feedback shift register (NLFSR) structure, utilizing S-box transformations and circular shifts for round key generation. In hardware implementations, LBlock achieves the same throughput as PRESENT-80 while occupying 16% less physical area, requiring only 1320 GE compared to 1570 GE. To enhance diffusion, the design processes half of the data per round while applying a simple rotation to the remaining half, balancing efficiency and security.

SIMON [140], designed by the NSA, is a lightweight block cipher optimized for both software and hardware implementations. A performance evaluation was presented in [140], demonstrating its efficiency across various platforms. It supports multiple key sizes (64, 72, 96, 128, 144, 192, 256 bits), block sizes (32, 48, 64, 96, 128 bits), and varying numbers of rounds (32, 36, 42, 44, 52, 54, 68, 69, 72). Its round function utilizes simple operations, including left circular shifts, AND, and XOR, enabling efficient circuit implementation while maintaining high performance in both software and hardware environments.

Simeck [141] is a hardware-oriented lightweight cipher designed to optimize both area efficiency and power consumption. It comprises three variants: Simeck-32/64, Simeck-48/96, and Simeck-64/128. The design integrates the strengths of SIMON and SPECK, adopting the round function of SIMON

while utilizing the key schedule of SPECK [140]. In hardware implementations, Simeck variants achieve the same throughput as their corresponding SIMON counterparts but with a more compact physical area and reduced power consumption [141], making them well-suited for resource-constrained environments.

SLIM [142] is an ultra-lightweight cipher with a 32-bit block size, an 80-bit key length, and 32 rounds. It utilizes four identical 4×4 S-boxes in its substitution layer, achieving a minimal hardware footprint of 553 GE, which is lower than that of SIMON-32/64 [140]. Similarly, LBC-IoT [143] is another ultra-lightweight cipher with the same block size, key length, and number of rounds as SLIM. It employs 4-bit S-boxes, shifts, and XOR operations to optimize hardware efficiency, requiring only 548 GE—making it even more compact than SLIM [143].

SCENERY [144], designed with a 64-bit block size, an 80-bit key, and 28 rounds, incorporates a round function consisting of eight parallel 4×4 S-boxes and a 32×32 binary diffusion matrix. In hardware implementations, it occupies 1438 GE, which is lower than both KLEIN-80 and PRESENT-80. On the other hand, LBCCS [145] features 20 rounds with a 128-bit block size and key length. It enhances security through highly robust S-boxes and diffusive P-boxes, leveraging combinational chaotic systems while reducing complexity via an extensible round function. However, its hardware implementation requires 2227 GE, which surpasses both DESXL and SCENERY.

3.3 Performance Evaluation Criteria

Lightweight ciphers are required to balance implementation cost and performance. In this section, the lightweight block ciphers are evaluated based on the following metrics:

Block Size, Key Size and Number of Rounds: Block ciphers operate by encrypting plaintext in fixed-size blocks, with smaller block sizes often favored in IoT devices due to their direct impact on computational and energy costs. Similarly, the cryptographic key size determines the balance between security and performance. Larger key sizes enhance security by increasing resistance to exhaustive key search attacks but come at the expense of greater computational complexity and energy consumption. The National Institute of Standards and Technology (NIST) recommends a minimum key size of 80 bits to ensure adequate security. Additionally, the security of lightweight block ciphers, which typically feature simpler structures than conventional ciphers,

https://doi.org/10.59222/ustjet.3.1.4

relies on multiple rounds of iteration. While increasing the number of rounds bolsters cryptanalysis resistance by ensuring that cryptanalysis complexity exceeds that of exhaustive key search attacks, it also reduces performance [146].

Gate Equivalent (GE) and Hardware technology: The physical area of a hardware implementation is measured in Gate Equivalents (GE), where one GE represents the area required for a single NAND2 gate in the corresponding technology. According to ISO/IEC standards [147], lightweight ciphers typically range between 1000 and 2000 GE. The occupied area of a cipher is influenced by the CMOS technology used for implementation, with commonly utilized technologies in Lightweight Cryptography (LWC) research being 0.13μm and 0.18μm. The GE metric quantifies the complexity and area of a hardware implementation by dividing its layout area in μm^2 by the area of a NAND2 gate in the same technology. For example, [148] reported that the PRESENT-80 cipher occupies 1075 GE in 0.18μm technology, 1169 GE in 0.25μm, and 1000 GE in 0.35μm, demonstrating the dependence of GE values on the underlying CMOS technology.

Latency and Throughput: Latency refers to the number of clock cycles required to process each plaintext or ciphertext block. In contrast, throughput (T) measures the number of bits encrypted or decrypted per second at a given frequency (F). The common hardware frequency is 100 kHz. throughput (T) is calculated using the formula:

$$T = \frac{F \times B}{N} \quad (1)$$

where (B) represents the block size in bits, and (N) denotes the number of clock cycles per block [75].

Efficiency: Efficiency evaluates the relationship between performance and implementation cost. Generally, higher efficiency values are preferable. Hardware efficiency $E_{hardware}$ [75] is calculated as:

$$\mathrm{E_{hardware}} = \frac{\mathrm{T}}{\mathrm{G}} \quad (2)$$

where T is throughput in kbps and G is GE in KGE. Similarly,

Power Requirement: Power represents the power consumption of implementation, typically in μW. For hardware implementation, it can be estimated from GE and hardware technology.

Energy Consumption: For hardware implementations, energy consumption per bit C_{bit} follows:

$$C_{bit} = \frac{P \times L}{B} \quad (3)$$

Where latency (L) is the number of clock cycles that are required to encrypt a block, power (P) is the μW that are consumed by the hardware implementation and block size (B) is the size of data in bits that each cipher can process in one encryption/decryption operation[75].

4. LWC Algorithms Performance Analysis and Discussion

In this survey paper, we compare hardware implementations for 43 lightweight block ciphers and evaluate the performance based on the criteria in the previous section. Table1 summarizes the search-related algorithms mentioned above according to the performance evaluation criteria described in Subsection 3.3.

Table 1: Summary of the Performance of the Hardware Implementations of 0.13 and 0.18 μm Hardware Technology Value

No.	Cipher	Year	Tech (μm)	Type	Key size (bits)	Block size (bits)	Rounds	Latency (Cycles/ block)	Throughput at 100 KHz (Kbps)	Area (GE)	Efficiency (Kbps/KGE)	Power (μW)	Energy (μJ / bit)
1	mCrypton [138]	2006	0.13	SPN	128	64	12	13	492.3	2949	166.93	3	6
2	mCrypton(E&D) [138]	2006	0.13	SPN	128	64	12	13	492.3	4108	119.83	4.1	8.34
3	mCrypton-64 [138]	2006	0.13	SPN	64	64	12	-	492.3	2420	203.43	-	-
4	mCrypton-96 [138]	2006	0.13	SPN	96	64	12	13	492.3	2681	183.62	2.68	5.45
5	TEA [163]	2006	0.18	Feistel	128	64	64	64	100	2355	42.46	3.53	35.32
6	DES [158]	2007	0.18	Feistel	56	64	16	144	44.4	2309	19.22	3.46	77.92
7	DESL [158]	2007	0.18	Feistel	56	64	16	144	44.4	1848	24.02	2.77	62.37
8	DESX(S) [158]	2007	0.18	Feistel	184	64	16	144	44.4	2629	16.88	3.94	88.72
9	PRESENT-128 [140]	2007	0.18	SPN	128	64	31	32	200	1886	106.04	2.82	14.14
10	PRESENT-80 [140]	2007	0.18	SPN	80	64	31	32	200	1570	127.38	2.35	11.77
11	ICEBERG [141]	2008	0.18	SPN	128	64	16	16	400	5817	68.76	8.72	21.81
12	XTEA [165]	2008	0.13	Feistel	128	64	64	32	200	2521	79.33	2.52	12.6
13	MIBS-64 [166]	2009	0.18	Feistel	64	64	32	32	200	1396	143.26	2.09	10.47
14	MIBS-80 [166]	2009	0.18	Feistel	80	64	32	32	200	1530	130.71	2.3	11.47
15	PUFFIN-2 [142]	2009	0.18	SPN	80	64	34	1240	5.2	1083	4.8	1.62	313.88
16	GOST [167]	2010	0.18	Feistel	256	64	32	264	24.24	651	37.23	0.97	40.28
17	PRINT-160[143]	2010	0.18	SPN	160	96	96	3072	3.13	726	4.31	1.09	348.48
18	PRINT-80 [143]	2010	0.18	SPN	80	48	48	768	6.25	402	15.54	0.6	96.48
19	AES [137]	2011	0.13	SPN	128	128	10	226	56.64	2400	23.6	2.4	42.38

https://doi.org/10.59222/ustjet.3.1.4

Table 1: Continued

No.	Cipher	Year	Tech (μm)	Type	Key size (bits)	Block size (bits)	Rounds	Latency (Cycles/ block)	Throughput at 100 KHz (Kbps)	Area (GE)	Efficiency (Kbps/KGE)	Power (μW)	Energy (μJ / bit)
20	EPCBC [144]	2011	0.18	SPN	96	96	32	792	12.12	1333	9.09	2	164.95
21	LBlock [135]	2011	0.18	Feistel	80	64	32	32	200	1320	151.51	2	9.9
22	LED-128 [145]	2011	0.18	SPN	128	64	32,48	1872	3.4	1265	2.68	1.89	555
23	LED-64 [145]	2011	0.18	SPN	64	64	32,48	1248	5.1	966	5.27	1.45	282.55
24	LED-80 [145]	2011	0.18	SPN	80	64	32,48	1872	3.4	1040	3.26	1.56	456.3
25	LED-96 [145]	2011	0.18	SPN	96	64	32,48	1872	3.4	1116	3.04	1.67	489.64
26	Klein-64 [130]	2012	0.18	SPN	64	64	12	207	30.9	1220	25.32	1.83	59.18
27	Klein-80 [130]	2012	0.18	SPN	80	64	16	271	23.62	1478	15.98	2.21	93.87
28	Klein-96 [130]	2012	0.18	SPN	96	64	20	335	19.1	1528	12.5	2.3	119.97
29	NOEKEON [147]	2012	0.18	SPN	128	128	16	3720	3.44	2862	1.2	4.3	1247.7
30	PRINCE [150]	2013	0.13	SPN	128	64	12	12	533.3	2953	180.6	2.95	5.53
31	SIMON [168]	2013	0.13	Feistel	128	128	68	559	22.9	1317	17.38	1.32	57.52
32	SIMON [168]	2013	0.13	Feistel	96	48	36	304	15.8	763	20.7	0.76	48.32
33	SIMON [168]	2013	0.13	Feistel	64	128	44	383	16.7	1000	16.7	1	59.84
34	RECTANGLE [153]	2014	0.13	SPN	128	64	25	26	246	1787	137.66	1.78	7.25
35	RECTANGLE [153]	2014	0.13	SPN	80	64	25	26	246	1467	167.68	1.46	5.96
36	Simeck [169]	2015	0.13	Feistel	128	64	44	383	16.7	958	17.43	0.96	57.45
37	PICO [154]	2016	0.18	SPN	128	64	32	-	-	1878	-	2.82	-
38	SKINNY [155]	2016	0.18	SPN	128	64	32	36	177.78	1696	104.82	2.54	14.29
39	SLIM [170]	2020	0.13	Feistel	80	32	32	160	20	553	36.17	0.55	27.5
40	LBC-IoT [171]	2021	0.13	Feistel	80	32	28	-	-	548	-	0.55	-
41	DULBC [156]	2022	0.13	SPN	128	64	29	-	-	1765	-	1.77	-
42	IVLBC [157]	2022	0.18	SPN	128	64	29	29	220.69	1668	132.31	2.5	11.33
43	SCENERY [172]	2022	0.18	Feistel	80	64	20	28	228.57	1438	158.95	2.16	9.45

To ensure a fair benchmarking process, the ciphers are categorized based on their target hardware technology and ranked within each category. For 0.13 μm hardware technology, Figures 3, 4, 5, and 6 rank the ciphers presented in Table 1 according to throughput, physical area, efficiency, and energy consumption, respectively.

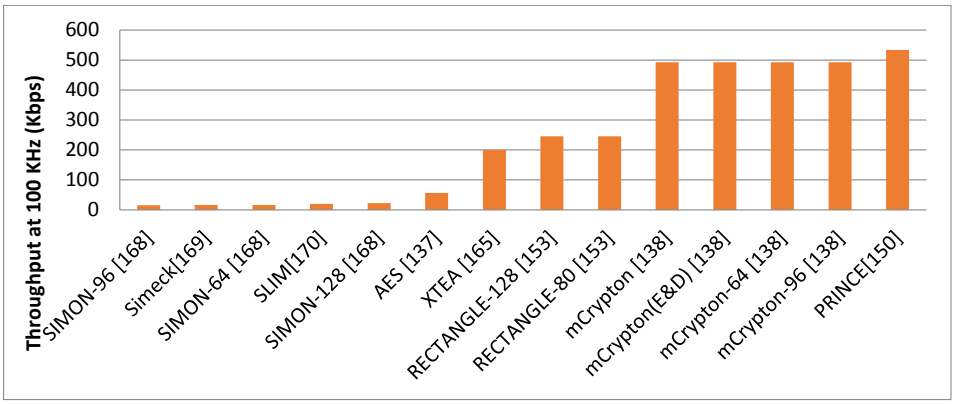

Figure 3: Throughput Ranking in 0.13 μm Hardware Implementations Technology

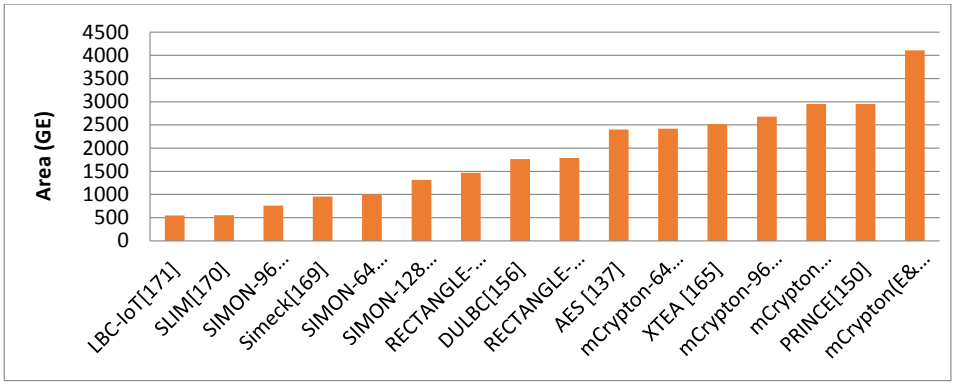

Figure 4: Physical Area Ranking in 0.13 μm Hardware Implementations Technology

https://doi.org/10.59222/ustjet.3.1.4

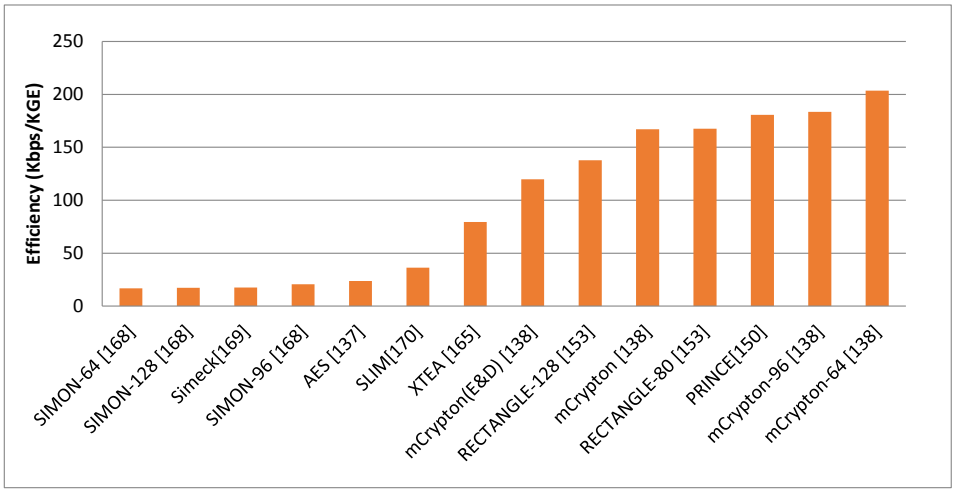

Figure 5: Hardware Efficiency Ranking in 0.13 μm Hardware Implementations Technology

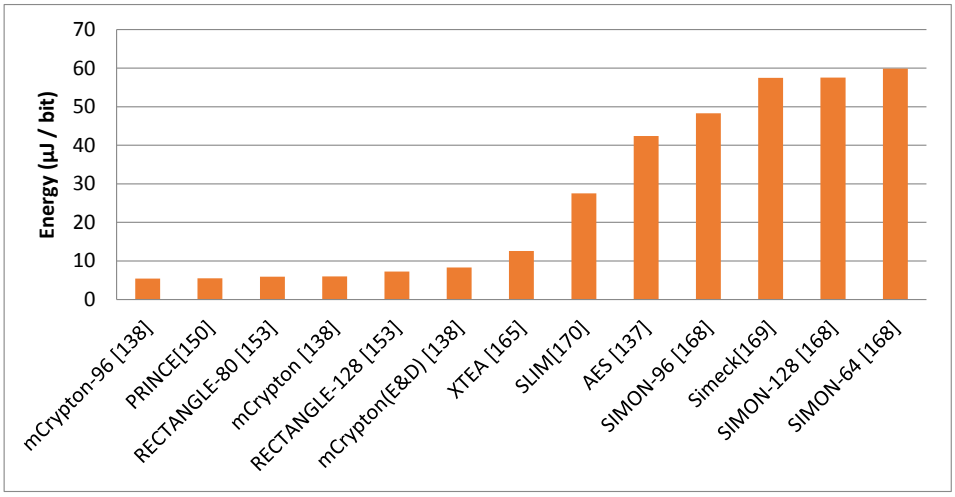

Figure 6: Energy Consumption Ranking in 0.13 μm Hardware Implementations Technology

For 0.18 μm hardware technology, Figures 7, 8, 9, and 10 rank the ciphers presented in Table 1 according to throughput, physical area, efficiency, and energy consumption, respectively.

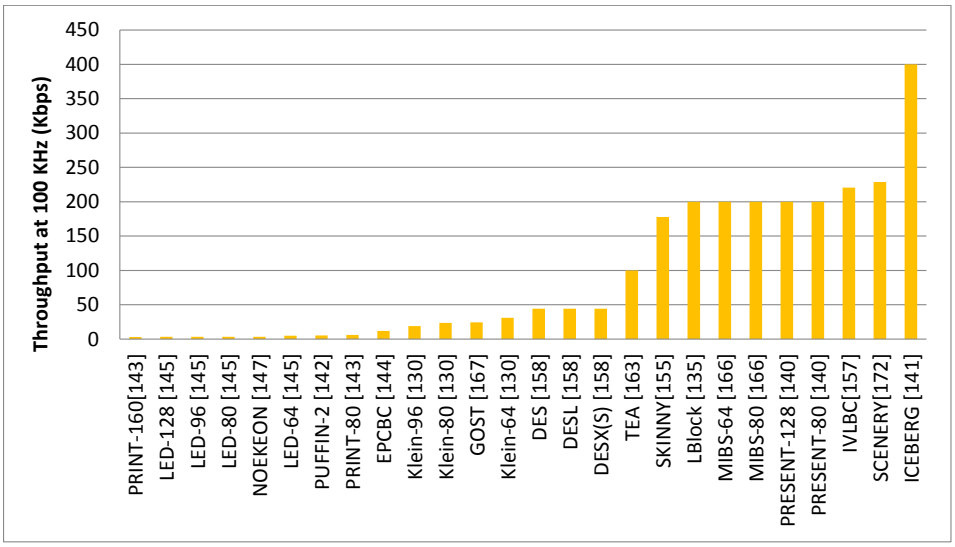

Figure 7: Throughput Ranking in 0.18 μm Hardware Implementations Technology

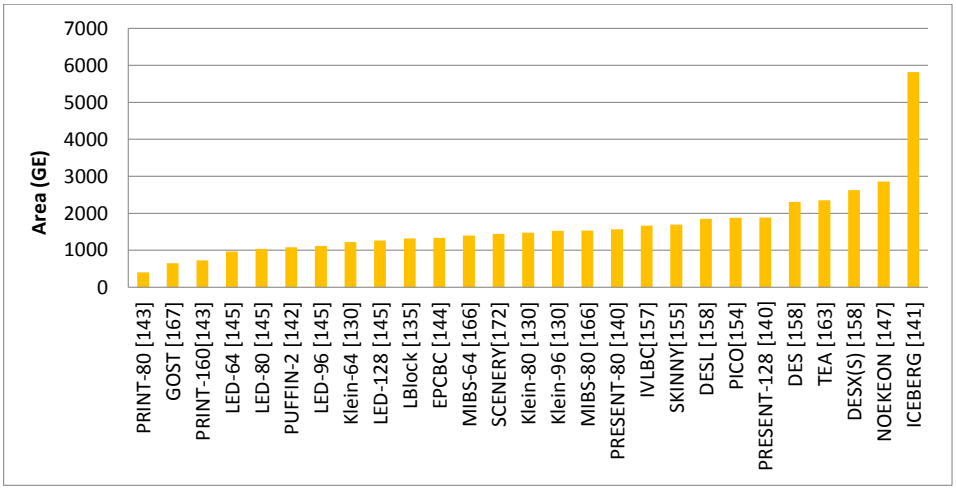

Figure 8: Physical Area Ranking in 0.18 μm Hardware Implementations Technology

https://doi.org/10.59222/ustjet.3.1.4

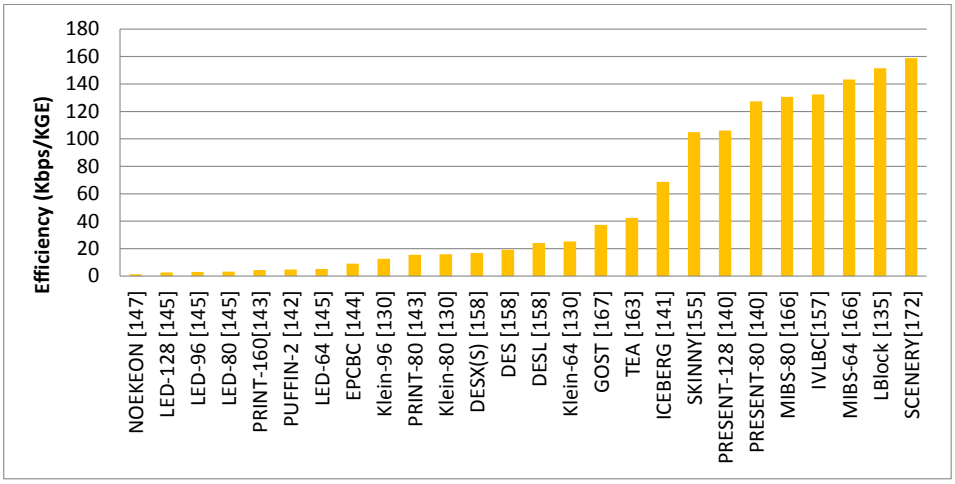

Figure 9: Hardware Efficiency Ranking in 0.18 μm Hardware Implementations Technology

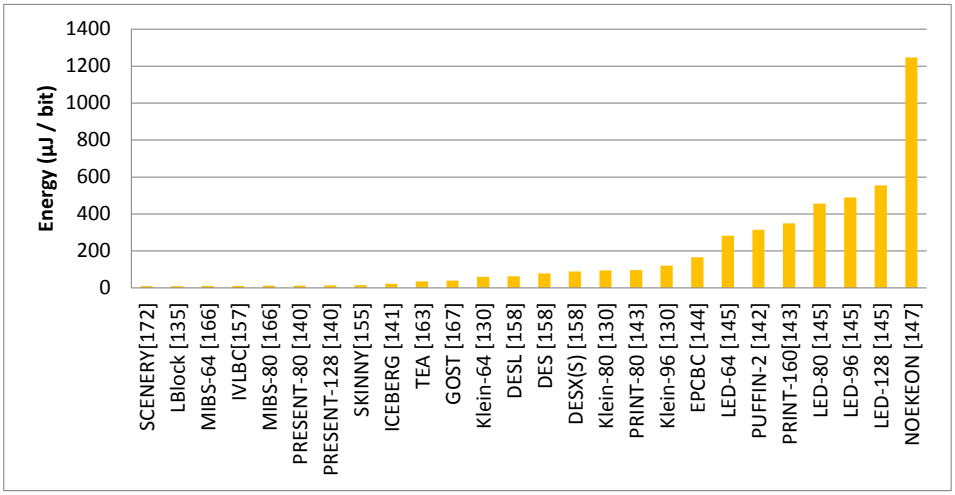

Figure 10: Energy Consumption Ranking in 0.18 μm Hardware Implementations Technology

From Table 1 and Figures 3 to 10 the following can be observed:

The key size and block size are fundamental parameters that influence both the security and efficiency of cryptographic algorithms. Larger key sizes, such as the 256-bit key used by GOST [167], 128-bit keys used by AES [137], and SIMON-128 [168], generally provide higher security but may require more

computational resources. In contrast, smaller key sizes, like the 56-bit key in DES [158] and the 64-bit key in mCrypton-64 [138], are more resource-efficient but may offer reduced security.

Similarly, the block size determines the amount of data processed in a single encryption operation. For example, AES [137], SIMON-128 [168], and NOEKEON [147] process 128-bit blocks, while most other ciphers, such as mCrypton [138], PRINCE [150], DES [158], and PRESENT-128 [140], process 64-bit blocks. Smaller block sizes, like the 32-bit blocks in LBC-IoT [171] and SLIM [170], are often more suitable for constrained devices but may compromise security.

The number of rounds in a cipher directly impacts its security and performance. More rounds typically enhance security but increase computational overhead. For instance, SIMON-128 [168] employs 68 rounds, significantly more than AES [137]›s 10 rounds, which contributes to its higher latency and energy consumption. Likewise, PRINT-160 [143] employs 96 rounds, significantly more than DES [158]›s 16 rounds.

Latency, measured in cycles per block, is a critical metric for real-time applications. Ciphers like mCrypton [138], PRINCE [150], ICEBERG [141] and LBlock [135] exhibit low latency (13, 12, 16 and 32 cycles per block, respectively), making them suitable for time-sensitive applications. In contrast, ciphers like SIMON-128 [168], Simeck [169], NOEKEON [147], and LED-128 [145] have higher latency, which may limit their use in real-time systems.

Throughput, measured in kilobits per second (Kbps) at a 100 KHz frequency, indicates the speed at which a cipher can process data. Higher throughput is desirable for high-speed applications. In 0.13 μm hardware technology, mCrypton [138] and its variants demonstrate high throughput (492.3 Kbps), making them efficient for data-intensive tasks. In contrast, ciphers like Simeck [169] and SIMON-128 [168] have significantly lower throughput (16.7 Kbps and 22.9 Kbps, respectively), which may restrict their use in high-speed environments. For 0.18 μm hardware technology, ICEBERG [141] demonstrates high throughput (400 Kbps). In contrast, ciphers like NOEKEON [147] and PRINT-160 [143] have significantly lower throughput (3.44 Kbps and 3.13 Kbps, respectively).

Efficiency, calculated as throughput per unit area (Kbps/KGE), reflects how effectively a cipher utilizes hardware resources. For 0.13 μm hardware technology, mCrypton-64 [138] stands out with the highest efficiency (203.43

https://doi.org/10.59222/ustjet.3.1.4

Kbps/KGE), indicating its optimization for hardware implementations. and in 0.18 μm hardware technology, SCENERY [172] stands out with the highest efficiency (158.95 Kbps/KGE).

The area metric, measured in Gate Equivalents (GE), represents the hardware footprint of a cipher. Smaller area ciphers are more suitable for resource-constrained devices. For example, LBC-IoT [171] has the smallest area (548 GE) in 0.13 μm hardware technology, and PRINT-80 [143] has the smallest area (402 GE) for 0.18 μm hardware technology, making it ideal for IoT applications.

Power consumption, measured in microwatts (μW), is another critical factor, especially for battery-operated devices. Ciphers like PRINT-80 [143], LBC-IoT[171], SLIM[170], and GOST [167] have the lowest power consumption (0.6 μW, 0.55 μW ,0.55μW and 0.97 μW, respectively), making them highly suitable for low-power applications.

Energy consumption, measured in (μJ/bit), is a crucial metric for energy-efficient designs. Lower values indicate more energy-efficient ciphers. In 0.13 μm hardware technology, mCrypton-96 [138] has the lowest energy consumption (5.45 μJ/bit), making it highly efficient for energy-sensitive applications. On the other hand, ciphers like SIMON-128 [168] and Simeck[169] have significantly higher energy consumption (57.52 μJ/bit and 57.45 μJ/bit, respectively), which may limit their use in energy-constrained environments. For 0.18 μm hardware technology, SCENERY [172] and LBlock [135] have the lowest energy consumption (9.45 μJ/bit and 9.9 μJ/bit, respectively). On the other hand, ciphers like NOEKEON [147] and LED-128 [145] have significantly higher energy consumption (1247.65 μJ/bit and 555 μJ/bit, respectively).

In summary, the analysis reveals that different ciphers excel in different metrics, and the choice of cipher depends on the specific requirements of the application. For instance, ICEBERG [141], IVLBC [157], mCrypton [138] and its variants offer a balanced combination of throughput, efficiency, and energy consumption, making them suitable for a wide range of applications. Conversely, ciphers like NOEKEON [147], LED-128 [145], SIMON-128 [168] and Simeck [169] may be more appropriate for applications where security is prioritized over speed and energy efficiency. Ultimately, the selection of a lightweight cryptographic algorithm should be guided by the trade-offs between security, performance, and resource constraints.

5. Conclusions

In conclusion, symmetric encryption, especially block ciphers, is ideal for resource-limited IoT environments. Among the various internal structures of block ciphers, SPN ciphers have shown greater resilience against security vulnerabilities. As a result, SPN ciphers are often the preferred choice in the field of LWC. This paper analyzed 43 lightweight block ciphers, evaluating their performance in terms of throughput, efficiency, energy use, and hardware area. The results highlight the trade-offs between security, performance, and resource efficiency, emphasizing the need to choose ciphers based on specific IoT application requirements. This study serves as a guide for researchers and developers, stressing the importance of lightweight cryptography in securing IoT and encouraging further innovation to meet emerging security challenges.

References

[1] H. Aldowah, S. U. Rehman, and I. Umar, "Security in internet of things: issues, challenges and solutions," in *International Conference of Reliable Information and Communication Technology*, 2018, pp. 396-405.

[2] E. Fernandes, A. Rahmati, K. Eykholt, and A. Prakash, "Internet of things security research: A rehash of old ideas or new intellectual challenges?," IEEE Security & Privacy, vol. 15, pp. 79-84, 2017.

[3] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet of things Journal*, vol. 4, pp. 1250-1258, 2017.

[4] Z. H. Ali, H. A. Ali, and M. M. Badawy, "Internet of Things (IoT): definitions, challenges and recent research directions," *International Journal of Computer Applications*, vol. 975, p. 8887, 2015.

[5] B. S. Ahmed, M. Bures, K. Frajtak, and T. Cerny, "Aspects of quality in Internet of Things (IoT) solutions: A systematic mapping study," *IEEE Access*, vol. 7, pp. 13758-13780, 2019.

[6] M. Usman, I. Ahmed, M. I. Aslam, S. Khan, and U. A. Shah, "SIT: a lightweight encryption algorithm for secure internet of things," *arXiv preprint arXiv:1704.08688*, 2017.

[7] J. S. Kumar and D. R. Patel, "A survey on internet of things: Security and privacy issues," *International Journal of Computer Applications*, vol. 90, 2014.

[8] D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for internet of things: A survey," *Journal of Network and Computer Applications*, vol. 66, pp. 198-213, 2016.

https://doi.org/10.59222/ustjet.3.1.4

[9] D. Evans, "The internet of things: How the next evolution of the internet is changing everything," *CISCO white paper*, vol. 1, pp. 1-11, 2011.

[10] M. Zolanvari and R. Jain, "IoT security: a survey," ed, 2015.

[11] B. Schneier, "IoT security: what's plan B?," *IEEE Security & Privacy*, pp. 96-96, 2017.

[12] Ericsson, "IoT security - protecting the networked society," *Ericsson White paper*, pp. 1-3, 2017.

[13] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer networks*, vol. 57, pp. 2266-2279, 2013.

[14] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer networks*, vol. 76, pp. 146-164, 2015.

[15] A. Jha and M. Sunil, "Security considerations for Internet of Things," *L&T Technology Services*, 2014.

[16] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in *2012 international conference on computer science and electronics engineering*, 2012, pp. 648-651.

[17] P. Wang, S. Chaudhry, L. Li, S. Li, T. Tryfonas, and H. Li, "The Internet of Things: a security point of view," *Internet Research*, 2016.

[18] M. Ebrahim, S. Khan, and U. Khalid, "Security risk analysis in peer 2 peer system; an approach towards surmounting security challenges," *arXiv preprint arXiv:1404.5123*, 2014.

[19] E. Perkins, "Securing the Internet of Things," *Gartner Research*, 2016.

[20] S. A. Kumar, T. Vealey, and H. Srivastava, "Security in internet of things: Challenges, solutions and future directions," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 2016, pp. 5772-5781.

[21] M. E. Forum, "The Impact of Trust on IoT."

[22] N. Perlroth, "Hackers Used New Weapons to Disrupt Major Websites Across U.S.," 2016.

[23] F. i. Intelligence, "Overload: Critical lessons from 15 years of ICSvulnerabilities," 2016.

[24] I. I. Consortium, "Industrial Internet of Things," vol. G4:Security Framework, 2016.

[25] S. B. Sadkhan and A. O. Salman, "A survey on lightweight-cryptography status and future challenges," in *2018 International Conference on Advance of Sustainable Engineering and its Application (ICASEA)*, 2018, pp. 105-108.

[26] Y. Harbi, Z. Aliouat, A. Refoufi, and S. Harous, "Recent security trends in internet of things: A comprehensive survey," *IEEE Access*, vol. 9, pp. 113292-113314, 2021.

[27] B. J. Mohd, T. Hayajneh, and A. V. Vasilakos, "A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues," *Journal of Network and Computer Applications*, vol. 58, pp. 73-93, 2015.

[28] T. Wollinger, J. Guajardo, and C. Paar, "Security on FPGAs: State-of-the-art implementations and attacks," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 3, pp. 534-574, 2004.

[29] O. Salhab, N. Jweihan, M. A. Jodeh, M. Abutaha, and M. Farajallah, "SURVEY PAPER: PSEUDO RANDOM NUMBER GENERATORS AND SECURITY TESTS," 2018.

[30] M. Bellare and P. Rogaway, "Optimal asymmetric encryption," in *Advances in Cryptology—EUROCRYPT'94: Workshop on the Theory and Application of Cryptographic Techniques Perugia, Italy, May 9–12, 1994 Proceedings 13*, 1995, pp. 92-111.

[31] G. J. Simmons, "Symmetric and asymmetric encryption," *ACM Computing Surveys (CSUR)*, vol. 11, pp. 305-330, 1979.

[32] M. Rana, Q. Mamun, and R. Islam, "Lightweight cryptography in IoT networks: A survey," *Future Generation Computer Systems*, vol. 129, pp. 77-89, 2022.

[33] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120-126, 1978.

[34] M. I. Mihailescu, S. L. Nita, M. I. Mihailescu, and S. L. Nita, "Cryptography Fundamentals," *Pro Cryptography and Cryptanalysis with C++ 20: Creating and Programming Advanced Algorithms*, pp. 15-63, 2021.

[35] C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, "Elliptic curve lightweight cryptography: A survey," *IEEE Access*, vol. 6, pp. 72514-72550, 2018.

[36] U. M. Maurer and S. Wolf, "The diffie–hellman protocol," *Designs, Codes and Cryptography*, vol. 19, pp. 147-171, 2000.

[37] D. Khleborodov, "Fast elliptic curve point multiplication based on binary and binary non-adjacent scalar form methods," *Advances in Computational Mathematics*, vol. 44, pp. 1275-1293, 2018.

https://doi.org/10.59222/ustjet.3.1.4

[38] D. Abbasinezhad-Mood and M. Nikooghadam, "Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications," *Future Generation Computer Systems*, vol. 84, pp. 47-57, 2018.

[39] A. Salman, A. Ferozpuri, E. Homsirikamol, P. Yalla, J.-P. Kaps, and K. Gaj, "A scalable ECC processor implementation for high-speed and lightweight with side-channel countermeasures," in *2017 international conference on ReConFigurable Computing and FPGAs (ReConFig)*, 2017, pp. 1-8.

[40] H. Hasan, T. Salah, D. Shehada, M. J. Zemerly, C. Y. Yeun, M. Al-Qutayri, et al., "Secure lightweight ECC-based protocol for multi-agent IoT systems," in *2017 IEEE 13th international conference on wireless and mobile computing, networking and communications (WiMob)*, 2017, pp. 1-8.

[41] Z. Liu, J. Weng, Z. Hu, and H. Seo, "Efficient elliptic curve cryptography for embedded devices," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 16, pp. 1-18, 2016.

[42] Z. Liu, X. Huang, Z. Hu, M. K. Khan, H. Seo, and L. Zhou, "On emerging family of elliptic curves to secure internet of things: ECC comes of age," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, pp. 237-248, 2016.

[43] K. Kaur, N. Kumar, M. Singh, and M. S. Obaidat, "Lightweight authentication protocol for RFID-enabled systems based on ECC," in *2016 IEEE global communications conference (GLOBECOM)*, 2016, pp. 1-6.

[44] D. He, H. Wang, M. K. Khan, and L. Wang, "Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography," *IET Communications*, vol. 10, pp. 1795-1802, 2016.

[45] J. Bosmans, S. S. Roy, K. Jarvinen, and I. Verbauwhede, "A tiny coprocessor for elliptic curve cryptography over the 256-bit NIST prime field," in *2016 29th International Conference on VLSI Design and 2016 15th International Conference on Embedded Systems (VLSID)*, 2016, pp. 523-528.

[46] S. Sinha Roy, K. Järvinen, and I. Verbauwhede, "Lightweight coprocessor for Koblitz curves: 283-bit ECC including scalar conversion with only 4300 gates," in *International workshop on cryptographic hardware and embedded systems*, 2015, pp. 102-122.

[47] D. B. Roy, P. Das, and D. Mukhopadhyay, "ECC on your fingertips: A single instruction approach for lightweight ECC design in gf (p)," in *International Conference on Selected Areas in Cryptography*, 2015, pp. 161-177.

[48] O. P. Pinol, S. Raza, J. Eriksson, and T. Voigt, "BSD-based elliptic curve cryptography for the open Internet of Things," in 2015 7th International Conference on New Technologies, *Mobility and Security (NTMS)*, 2015, pp. 1-5.

[49] A. Höller, N. Druml, C. Kreiner, C. Steger, and T. Felicijan, "Hardware/software co-design of elliptic-curve cryptography for resource-constrained applications," in *Proceedings of the 51st Annual Design Automation Conference*, 2014, pp. 1-6.

[50] N. Druml, M. Menghin, A. Kuleta, C. Steger, R. Weiss, H. Bock, et al., "A flexible and lightweight ECC-based authentication solution for resource constrained systems," in *2014 17th Euromicro Conference on Digital System Design*, 2014, pp. 372-378.

[51] R. Azarderakhsh, K. U. Järvinen, and M. Mozaffari-Kermani, "Efficient algorithm and architecture for elliptic curve cryptography for extremely constrained secure applications," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 61, pp. 1144-1155, 2014.

[52] E. Wenger, T. Korak, and M. Kirschbaum, "Analyzing side-channel leakage of RFID-suitable lightweight ECC hardware," in *Radio Frequency Identification: Security and Privacy Issues 9th International Workshop*, RFIDsec 2013, Graz, Austria, July 9-11, 2013, Revised Selected Papers 9, 2013, pp. 128-144.

[53] E. Wenger, "A lightweight ATmega-based application-specific instruction-set processor for elliptic curve cryptography," in *Lightweight Cryptography for Security and Privacy: Second International Workshop*, LightSec 2013, Gebze, Turkey, May 6-7, 2013, Revised Selected Papers 2, 2013, pp. 1-15.

[54] E. Wenger, "Hardware architectures for MSP430-based wireless sensor nodes performing elliptic curve cryptography," in *Applied Cryptography and Network Security: 11th International Conference*, ACNS 2013, Banff, AB, Canada, June 25-28, 2013. Proceedings 11, 2013, pp. 290-306.

[55] M. Schramm and A. Grzemba, "On the implementation of a lightweight generic FPGA ECC crypto-core over GF (p)," in *2013 International Conference on Applied Electronics*, 2013, pp. 1-4.

[56] S. Namal, K. Georgantas, and A. Gurtov, "Lightweight authentication and key management on 802.11 with Elliptic Curve Cryptography," in *2013 IEEE Wireless Communications and Networking Conference (WCNC)*, 2013, pp. 1830-1835.

[57] E. Wenger and J. Grossschadl, "An 8-bit AVR-based elliptic curve cryptographic RISC processor for the internet of things," in *2012 45th Annual IEEE/ACM International Symposium on Microarchitecture Workshops*, 2012, pp. 39-46.

https://doi.org/10.59222/ustjet.3.1.4

[58] V. Trujillo-Olaya, T. Sherwood, and Ç. K. Koç, "Analysis of performance versus security in hardware realizations of small elliptic curves for lightweight applications," *Journal of Cryptographic Engineering*, vol. 2, pp. 179-188, 2012.

[59] M. Varchola, T. Guneysu, and O. Mischke, "MicroECC: A lightweight reconfigurable elliptic curve crypto-processor," in *2011 International Conference on Reconfigurable Computing and FPGAs*, 2011, pp. 204-210.

[60] M. Abujoodeh, L. Tamimi, and R. Tahboub, "Toward Lightweight Cryptography: A Survey," in *Computational Semantics*, ed: IntechOpen, 2023.

[61] M. Rana and Q. Mamun, "A robust and lightweight key management protocol for WSNs in distributed IoT applications," *International Journal of Systems and Software Security and Protection (IJSSSP)*, vol. 9, pp. 1-16, 2018.

[62] N. M. Naser and J. R. Naif, "A systematic review of ultra-lightweight encryption algorithms," I*nternational Journal of Nonlinear Analysis and Applications*, vol. 13, pp. 3825-3851, 2022.

[63] N. A. Mohandas, A. Swathi, R. Abhijith, A. Nazar, and G. Sharath, "A4: A lightweight stream cipher," in *2020 5th International Conference on Communication and Electronics Systems (ICCES)*, 2020, pp. 573-577.

[64] H. Noura, R. Couturier, C. Pham, and A. Chehab, "Lightweight stream cipher scheme for resource-constrained IoT devices," in *2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2019, pp. 1-8.

[65] L. Ding, C. Liu, Y. Zhang, and Q. Ding, "A new lightweight stream cipher based on chaos," *Symmetry*, vol. 11, p. 853, 2019.

[66] M. Agren, M. Hell, T. Johansson, and W. Meier, "A new version of grain-128 with authentication," in *Symmetric Key Encryption Workshop*, 2011.

[67] C. De Canniere, "Trivium: A stream cipher construction inspired by block cipher design principles," in *International Conference on Information Security*, 2006, pp. 171-186.

[68] M. Hell, T. Johansson, A. Maximov, W. Meier, J. Sönnerup, and H. Yoshida, "Grain-128AEADv2-A lightweight AEAD stream cipher," *Submission to NIST LWC Project*, 2021.

[69] M. Hell, T. Johansson, and W. Meier, "Grain: a stream cipher for constrained environments," *International journal of wireless and mobile computing*, vol. 2, pp. 86-93, 2007.

[70] D. Watanabe, T. Owada, K. Okamoto, Y. Igarashi, and T. Kaneko, "Update on enocoro stream cipher," in *2010 International Symposium On Information Theory & Its Applications*, 2010, pp. 778-783.

[71] A. Srivastava and A. Kumar, "A review on authentication protocol and ECC in IoT," in *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 2021, pp. 312-319.

[72] C. Tezcan, "The improbable differential attack: Cryptanalysis of reduced round CLEFIA," in *Progress in Cryptology-INDOCRYPT 2010: 11th International Conference on Cryptology in India*, Hyderabad, India, December 12-15, 2010. Proceedings 11, 2010, pp. 197-209.

[73] D. Watanabe, K. Ideguchi, J. Kitahara, K. Muto, H. Furuichi, and T. Kaneko, "Enocoro-80: A hardware oriented stream cipher," in *2008 Third International Conference on Availability, Reliability and Security*, 2008, pp. 1294-1300.

[74] C. E. Shannon, "Communication theory of secrecy systems," *The Bell system technical journal*, vol. 28, pp. 656-715, 1949.

[75] G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou, and C. Manifavas, "A review of lightweight block ciphers," *Journal of cryptographic Engineering*, vol. 8, pp. 141-184, 2018.

[76] R. Kousalya and G. S. Kumar, "A survey of light-weight cryptographic algorithm for information security and hardware efficiency in resource constrained devices," in *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)*, 2019, pp. 1-5.

[77] M. Cazorla, S. Gourgeon, K. Marquet, and M. Minier, "Survey and benchmark of lightweight block ciphers for MSP430 16-bit microcontroller," *Security and communication networks*, vol. 8, pp. 3564-3579, 2015.

[78] R. Hamza, Z. Yan, K. Muhammad, P. Bellavista, and F. Titouna, "A privacy-preserving cryptosystem for IoT E-healthcare," *Information Sciences*, vol. 527, pp. 493-510, 2020.

[79] V. Prakash, A. V. Singh, and S. K. Khatri, "A new model of light weight hybrid cryptography for internet of things," in *2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA)*, 2019, pp. 282-285.

[80] A. P. R. Da Silva, M. H. Martins, B. P. Rocha, A. A. Loureiro, L. B. Ruiz, and H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," in *Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*, 2005, pp. 16-23.

https://doi.org/10.59222/ustjet.3.1.4

[81] C. Zhao, Y. Yan, and W. Li, "An efficient ASIC implementation of QARMA lightweight algorithm," in *2019 IEEE 13th International Conference on ASIC (ASICON)*, 2019, pp. 1-4.

[82] M. J. R. Shantha and L. Arockiam, "Sat_Jo: an enhanced lightweight block cipher for the internet of things," in *2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS)*, 2018, pp. 1146-1150.

[83] Z. M. J. Kubba and H. K. Hoomod, "A hybrid modified lightweight algorithm combined of two cryptography algorithms PRESENT and Salsa20 using chaotic system," in *2019 First International Conference of Computer and Applied Sciences (CAS)*, 2019, pp. 199-203.

[84] H. Noura, A. Chehab, L. Sleem, M. Noura, R. Couturier, and M. M. Mansour, "One round cipher algorithm for multimedia IoT devices," *Multimedia tools and applications*, vol. 77, pp. 18383-18413, 2018.

[85] H. Noura, A. Chehab, and R. Couturier, "Lightweight dynamic key-dependent and flexible cipher scheme for IoT devices," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, 2019, pp. 1-8.

[86] R. R. K. Chaudhary and K. Chatterjee, "An efficient lightweight cryptographic technique for IoT based E-healthcare system," in *2020 7th International Conference on Signal Processing and Integrated Networks (SPIN)*, 2020, pp. 991-995.

[87] A. Alahdal, G. A. AL-Rummana, G. Shinde, and N. K. Deshmukh, "NLBSIT: A new lightweight block cipher design for securing data in IOT devices," *International Journal of Computer Sciences and Engineering*, vol. 8, 2020.

[88] V. Amin Ghafari and H. Hu, "Fruit-80: a secure ultra-lightweight stream cipher for constrained environments," *Entropy*, vol. 20, p. 180, 2018.

[89] G. Bansod, A. Patil, S. Sutar, and N. Pisharoty, "ANU: an ultra lightweight cipher design for security in IoT," *Security and Communication Networks*, vol. 9, pp. 5238-5251, 2016.

[90] G. Bansod, N. Pisharoty, and A. Patil, "BORON: an ultra-lightweight and low power encryption design for pervasive computing," *Frontiers of Information Technology & Electronic Engineering*, vol. 18, pp. 317-331, 2017.

[91] M. Bokhari and S. Hassan, "A comparative study on lightweight cryptography," in *Cyber Security: Proceedings of CSI 2015*, 2018, pp. 69-79.

[92] H. Cheng, H. M. Heys, and C. Wang, "Puffin: A novel compact block cipher targeted to embedded digital systems," in *2008 11th EUROMICRO Conference on Digital System Design Architectures, Methods and Tools*, 2008, pp. 383-390.

[93] V. Dahiphale, G. Bansod, and J. Patil, "ANU-II: A fast and efficient lightweight encryption design for security in IoT," in *2017 International Conference on Big Data, IoT and Data Science (BID)*, 2017, pp. 130-137.

[94] A. B. Dar, M. J. Lone, and N. Hussain, "Revisiting lightweight block ciphers: review, taxonomy and future directions," *Computer Science Review, Forthcoming*, 2021.

[95] L. Ertaul and S. K. Rajegowda, "Performance analysis of CLEFIA, PICCOLO, TWINE Lightweight block ciphers in IoT environment," in *Proceedings of the International Conference on Security and Management (SAM)*, 2017, pp. 25-31.

[96] Z. Gong, S. Nikova, and Y. W. Law, "KLEIN: a new family of lightweight block ciphers," in *International workshop on radio frequency identification: security and privacy issues*, 2011, pp. 1-18.

[97] L. Li, B. Liu, and H. Wang, "QTL: a new ultra-lightweight block cipher," *Microprocessors and Microsystems*, vol. 45, pp. 45-55, 2016.

[98] J. Patil, G. Bansod, and K. S. Kant, "LiCi: A new ultra-lightweight block cipher," in *2017 International Conference on Emerging Trends & Innovation in ICT (ICEI)*, 2017, pp. 40-45.

[99] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shirai, "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*, 2011, pp. 342-357.

[100] T. Suzaki, K. Minematsu, S. Morioka, and E. Kobayashi, "Twine: A lightweight, versatile block cipher," in *ECRYPT workshop on lightweight cryptography*, 2011.

[101] W. Wu and L. Zhang, "LBlock: a lightweight block cipher," in *Applied Cryptography and Network Security: 9th International Conference, ACNS 2011, Nerja, Spain, June 7-10, 2011. Proceedings 9, 2011*, pp. 327-344.

[102] W. Zhang, Z. Bao, D. Lin, V. Rijmen, B. Yang, and I. Verbauwhede, "RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms," *Cryptology ePrint Archive*, 2014.

https://doi.org/10.59222/ustjet.3.1.4

[103] A. Moradi, A. Poschmann, S. Ling, C. Paar, and H. Wang, "Pushing the limits: A very compact and a threshold implementation of AES," in *Advances in Cryptology–EUROCRYPT 2011: 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings 30*, 2011, pp. 69-88.

[104] M. James and D. S. Kumar, "An implementation of modified lightweight advanced encryption standard in FPGA," *Procedia Technology*, vol. 25, pp. 582-589, 2016.

[105] A. Nemati, S. Feizi, A. Ahmadi, S. Haghiri, M. Ahmadi, and S. Alirezaee, "An efficient hardware implementation of few lightweight block cipher," in *2015 The International Symposium on Artificial Intelligence and Signal Processing (AISP)*, 2015, pp. 273-278.

[106] W. Yu and S. Köse, "A lightweight masked AES implementation for securing IoT against CPA attacks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, pp. 2934-2944, 2017.

[107] J. Vimalkumar, H. R. Babu, and M. Bhaskar, "FPGA Implementation of Modified Lightweight 128-Bit AES Algorithm for IoT Applications," in *2023 IEEE International Symposium on Smart Electronic Systems (iSES)*, 2023, pp. 306-309.

[108] A. T. Abebe, "Lightweight and Efficient Architecture for AES Algorithm based on FPGA," *i-ETC: ISEL Academic Journal of Electronics Telecommunications and Computers*, vol. 8, 2023.

[109] M. M. Wong, D. M. Wong, C. Zhang, and I. Hijazin, "Circuit and system design for optimal lightweight AES encryption on FPGA," 2018.

[110] C. H. Lim and T. Korkishko, "mCrypton–a lightweight block cipher for security of low-cost RFID tags and sensors," in *International workshop on information security applications*, 2005, pp. 243-258.

[111] C. H. Lim, "A revised version of CRYPTON: CRYPTON V1. 0," in *International Workshop on Fast Software Encryption*, 1999, pp. 31-45.

[112] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, et al., "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*, 2007, pp. 450-466.

[113] H. Cheng and H. M. Heys, "Compact ASIC implementation of the ICEBERG block cipher with concurrent error detection," in *2008 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2008, pp. 2921-2924.

[114] C. Wang and H. M. Heys, "An ultra compact block cipher for serialized architecture implementations," in *2009 Canadian Conference on Electrical and Computer Engineering*, 2009, pp. 1085-1090.

[115] L. Knudsen, G. Leander, A. Poschmann, and M. J. Robshaw, "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*, 2010, pp. 16-32.

[116] H. Yap, K. Khoo, A. Poschmann, and M. Henricksen, "EPCBC-a block cipher suitable for electronic product code encryption," in *Cryptology and Network Security: 10th International Conference, CANS 2011, Sanya, China, December 10-12, 2011. Proceedings 10*, 2011, pp. 76-97.

[117] J. Guo, T. Peyrin, A. Poschmann, and M. Robshaw, "The LED block cipher," in *Cryptographic Hardware and Embedded Systems–CHES 2011: 13th International Workshop, Nara, Japan, September 28–October 1, 2011. Proceedings 13*, 2011, pp. 326-341.

[118] J. Guo, T. Peyrin, and A. Poschmann, "The PHOTON family of lightweight hash functions," in *Advances in Cryptology–CRYPTO 2011: 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings 31*, 2011, pp. 222-239.

[119] J. Daemen, M. Peeters, G. Assche, and V. Rijmen, "The noekeon block cipher," in *First Open NESSIE workshop*, 2000.

[120] J. Daemen, M. Peeters, G. Van Assche, and V. Rijmen, "Nessie proposal: NOEKEON," in *First open NESSIE workshop*, 2000, pp. 213-230.

[121] T. Plos, C. Dobraunig, M. Hofinger, A. Oprisnik, C. Wiesmeier, and J. Wiesmeier, "Compact hardware implementations of the block ciphers mCrypton, NOEKEON, and SEA," in *Progress in Cryptology-INDOCRYPT 2012: 13th International Conference on Cryptology in India, Kolkata, India, December 9-12, 2012. Proceedings 13*, 2012, pp. 358-377.

[122] J. Borgho, A. Canteaut, T. Guneysu, E. Kavun, M. Knezevic, L. Knudsen, et al., "Prince-a low-latency block cipher for pervasive computing applications-proc. of advances in cryptology," ed: LNCS, 2012.

[123] L. Batina, A. Das, B. Ege, E. B. Kavun, N. Mentens, C. Paar, et al., "Dietary recommendations for lightweight block ciphers: power, energy and area analysis of recently developed architectures," in *Radio Frequency Identification: Security and Privacy Issues 9th International Workshop, RFIDsec 2013, Graz, Austria, July 9-11, 2013, Revised Selected Papers 9*, 2013, pp. 103-112.

https://doi.org/10.59222/ustjet.3.1.4

[124] M. R. Z'aba, N. Jamil, M. E. Rusli, M. Z. Jamaludin, and A. A. M. Yasir, "I-present tm: An involutive lightweight block cipher," *Journal of Information Security*, vol. 2014, 2014.

[125] W. Zhang, Z. Bao, D. Lin, V. Rijmen, B. Yang, and I. Verbauwhede, "RECTANGLE: A Bit-slice Ultra-Lightweight Block Cipher Suitable for Multiple Platforms," *IACR Cryptol. ePrint Arch.*, vol. 2014, pp. 84-84, 2014.

[126] G. Bansod, N. Pisharoty, and A. Patil, "PICO: An ultra lightweight and low power encryption design for ubiquitous computing," *Defence Science Journal*, vol. 66, pp. 259-265, 2016.

[127] C. Beierle, J. Jean, S. Kölbl, G. Leander, A. Moradi, T. Peyrin, et al., "The SKINNY family of block ciphers and its low-latency variant MANTIS," in *Advances in Cryptology–CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II 36*, 2016, pp. 123-153.

[128] J. Yang, L. Li, Y. Guo, and X. Huang, "DULBC: A dynamic ultra-lightweight block cipher with high-throughput," *Integration*, vol. 87, pp. 221-230, 2022.

[129] X. Huang, L. Li, and J. Yang, "IVLBC: An involutive lightweight block cipher for Internet of Things," *IEEE Systems Journal*, vol. 17, pp. 3192-3203, 2022.

[130] G. Leander, C. Paar, A. Poschmann, and K. Schramm, "New lightweight DES variants," in *Fast Software Encryption: 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers 14*, 2007, pp. 196-210.

[131] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, et al., "Camellia: A 128-bit block cipher suitable for multiple platforms—design andanalysis," in *Selected Areas in Cryptography: 7th Annual International Workshop, SAC 2000 Waterloo, Ontario, Canada, August 14–15, 2000 Proceedings 7*, 2001, pp. 39-56.

[132] A. Satoh and S. Morioka, "Hardware-focused performance comparison for the standard block ciphers aes, camellia, and triple-des," in *Information Security: 6th International Conference, ISC 2003, Bristol, UK, October 1-3, 2003. Proceedings 6*, 2003, pp. 252-266.

[133] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, "The 128-bit blockcipher CLEFIA," in *Fast Software Encryption: 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers 14*, 2007, pp. 181-195.

[134] T. Akishita and H. Hiwatari, "Very compact hardware implementations of the blockcipher CLEFIA," in *Selected Areas in Cryptography: 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11-12, 2011, Revised Selected Papers 18*, 2012, pp. 278-292.

[135] D. J. Wheeler and R. M. Needham, "TEA, a tiny encryption algorithm," in *Fast Software Encryption: Second International Workshop Leuven, Belgium, December 14–16, 1994 Proceedings 2*, 1995, pp. 363-366.

[136] Y. Yu, Y. Yang, Y. Fan, and H. Min, "Security scheme for RFID tag," *Auto-ID Labs Fudan University, White Paper*, 2006.

[137] J.-P. Kaps, "Chai-tea, cryptographic hardware implementations of xtea," in *Progress in Cryptology-INDOCRYPT 2008: 9th International Conference on Cryptology in India, Kharagpur, India, December 14-17, 2008. Proceedings 9*, 2008, pp. 363-375.

[138] M. Izadi, B. Sadeghiyan, S. S. Sadeghian, and H. A. Khanooki, "MIBS: A new lightweight block cipher," in *International Conference on Cryptology and Network Security*, 2009, pp. 334-348.

[139] A. Poschmann, S. Ling, and H. Wang, "256 bit standardized crypto for 650 GE–GOST revisited," in *International Workshop on Cryptographic Hardware and Embedded Systems*, 2010, pp. 219-233.

[140] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK lightweight block ciphers," in *Proceedings of the 52nd annual design automation conference*, 2015, pp. 1-6.

[141] G. Yang, B. Zhu, V. Suder, M. D. Aagaard, and G. Gong, "The simeck family of lightweight block ciphers," in *International workshop on cryptographic hardware and embedded systems*, 2015, pp. 307-329.

[142] B. Aboushosha, R. A. Ramadan, A. D. Dwivedi, A. El-Sayed, and M. M. Dessouky, "SLIM: A lightweight block cipher for internet of health things," *IEEE Access*, vol. 8, pp. 203747-203757, 2020.

[143] R. A. Ramadan, B. W. Aboshosha, K. Yadav, I. M. Alseadoon, M. J. Kashout, and M. Elhoseny, "LBC-IoT: Lightweight Block Cipher for IoT Constraint Devices," *Computers, Materials & Continua*, vol. 67, 2021.

[144] J. Feng and L. Li, "SCENERY: a lightweight block cipher based on Feistel structure," *Frontiers of Computer Science*, vol. 16, p. 163813, 2022.

[145] D. Zhu, X. Tong, Z. Wang, and M. Zhang, "A novel lightweight block encryption algorithm based on combined chaotic system," *Journal of Information Security and Applications*, vol. 69, p. 103289, 2022.

https://doi.org/10.59222/ustjet.3.1.4

[146] Y. Zhong and J. Gu, "Lightweight block ciphers for resource-constrained environments: A comprehensive survey," *Future Generation Computer Systems*, 2024.

[147] C. Pei, Y. Xiao, W. Liang, and X. Han, "Trade-off of security and performance of lightweight block ciphers in Industrial Wireless Sensor Networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, pp. 1-18, 2018.

[148] C. Rolfes, A. Poschmann, G. Leander, and C. Paar, "Ultra-lightweight implementations for smart devices–security for 1000 gate equivalents," in *Smart Card Research and Advanced Applications: 8th IFIP WG 8.8/11.2 International Conference, CARDIS 2008, London, UK, September 8-11, 2008. Proceedings 8*, 2008, pp. 89-103.