International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(22s) 2026 pp. 69-80
https://doi.org/10.70917/ijcisim-2026-5419
Article

A Comprehensive Survey on Light weight block Ciphers with Authentication approaches for low resource IoT devices

Chaitra P[1], Dr Shobha I Hugar[2]

[1]Dept. of Computer Science and Engineering Atria Institute of Technology, Bangalore, India
[2]Dept of Electronics and Communication Engineering Sapthagiri College of Engineering, Bangalore, India

Abstract: Resource limited devices like IoT nodes, RFID tags, wireless sensor networks, and embedded edge technologies can now be safeguarded with the help of lightweight cryptography. Traditional cryptographic primitives are not suitable for these devices because they work under stringent conditions on power, area, storage, and latency. With emphasis on hardware implementations, this review offers an in depth and methodical analysis of existing lightweight block ciphers and authentication techniques. High-profile journal articles published between 2018 and 2026 are scrutinized and analyzed using a PRISMA-based methodology. The study includes techniques that are focused on authentication as well as traditional and new lightweight block ciphers. Metrics at the ASIC and FPGA levels, including LUTs, power usage, frequency, slices, latency, throughput, and hardware efficiency, are used to perform quantitative comparisons. Significant design trade-offs between area-optimized, throughput-oriented, and energy-efficient designs are highlighted in the analysis, along with the increasing trend of integrated encryption–authentication approaches. The survey also finds inadequacies in side-channel resilience, scalability across various heterogeneous platforms, security–efficiency co-optimization, and uniform benchmarking. Finally, future research scope is described for leading the creation of emerging lightweight cryptographic architectures that strike a undermine between hardware efficiency and robustness for contexts with limited resources.
Keywords: Lightweight Block ciphers, IoT, Throughput, FPGA, ASIC, Authentication

1. INTRODUCTION

Research on Internet of Things (IoT) security is subject to intense discussion. IoT is an interconnected paradigm that turns commonplace objects into smart devices by utilizing sensors and Internet technologies. With the help of these gadgets, users may access a variety of services at any time and from any location utilizing any kind of communication. Therefore, digitization is no longer a choice when it comes to our everyday activities, such as wearables, e-health, intelligent homes, intelligent cities, etc. Because IoT endpoints

frequently operate in insecure contexts, there are several security issues that need to be considered [1].

Lightweight block ciphers (LWBCs) have been an important field of study and development to address these issues. By reducing gate area, power usage, and computational difficulty while maintaining a respectable degree of cryptographic security, LWBCs are made to satisfy the demanding specifications of limited devices. Secure data transfer, device authentication, and safeguarding privacy are just a few of the uses for these ciphers [2]. The necessity for extensible security measures, the constraints of

conventional encryption standards in constrained locations, and the growing threat of assaults on ubiquitous technology have all contributed to the development of LWBCs. Numerous structural strategies, including Feistel networks, substitution-permutation networks (SPNs), and generalized Feistel networks (GFNs), have been suggested by researchers as LWBCs. These approaches frequently incorporate special optimization strategies for contexts [3].

The NIST launched the Lightweight Cryptography (LWC) initiative in 2013 to optimize safety and efficiency for gadgets with limited resources. NIST and other experts examine the effectiveness of current cryptographic specifications and work to create alternative lightweight cryptography protocols as part of the LWC initiative. Among the NIST's demands, a comprehensive algorithm description and standard implementations are crucial. The algorithms, associated computations, equations, design choices, and a design justification must all be included in the technical report [4]. An authentication procedure may need the user to interact physically or remotely, contingent upon the use scenario. As a result, multiple use cases result in multiple authentication methods with different purposes and objectives. The investigations could be categorized according to the expenses and security needs. Cryptographic primitives, application domains, spatiality of accessibility, and authentication criteria could all be used to discuss the research' safety necessities and capabilities. Costs could be examined according to hardware utilization, processing, and connectivity. Therefore, whether the research could be adequate and effective for connected devices [5-7]. Image encryption has become one of the most important methods for protecting visual data in fields like mobile devices, medical care, and monitoring [8].

The security and effectiveness of the encryption technique are assessed using a few metrics and factors that determine the quality of Image encryption. Additionally, processing time is another issue to consider, which suggests that an efficient encryption method is required [9–10].

Problem statement: The need for reliable connection under extreme hardware and energy restrictions has increased due to the quick spread of IoT and cyber-physical systems. Although many lightweight block ciphers and authentication methods have been put out, their designs are frequently assessed separately using disparate platforms, metrics, and presumptions. It is challenging to assess security effectiveness, hardware cost, and efficiency trade-offs amongst solutions objectively because of this fragmentation. Furthermore, a lot of current research focuses

on either authentication resilience or encryption effectiveness, with little attention paid to integrated authenticated encryption appropriate for limited hardware. A lack of scalability among FPGA and ASIC systems, uneven benchmarking techniques, and insufficient assessment of power and side-channel assaults are further issues. A comprehensive, hardware-focused survey that methodically examines current lightweight block ciphers and authentication techniques, evaluates their implementation-level outcomes, and pinpoints research gaps impeding their practical deployment in low-resource practical devices is therefore desperately needed.

Contribution: The primary contributions of the review work are listed as follows: The work offers a comprehensive PRISMA-based analysis of new lightweight block ciphers and authentication methods for devices with limited resources that were released between 2018 and 2025. The work offers a thorough comparison of FPGA/ASIC implementations based on hardware parameters such as area, LUTs, frequency, power, latency, throughput, and hardware efficiency. Examines and evaluates lightweight cryptography methods based on authentication in terms of hardware performance, computational complexity, and security. Highlights the way various hardware architectures affect performance by identifying design trends and trade-offs across lightweight cryptographic algorithms. The work identifies important research gaps and also outlines future research routes toward unified, adaptive, and secure lightweight cryptographic architectures for edge computing, IoT, WSN, and RFID applications.

The organization of the article is as follows: Section II covers the methodology adapted for review work and recent existing works on lightweight ciphers and authentication approaches. Section III discusses the results and analysis, including the comparison of architecture-based approaches, and future research directions. Lastly, the conclusion of the overall work is in section IV.

2. METHODOLOGY

The PRISMA-based systematic literature review approach is described in Fig.1 and it is organized and transparent procedure for identifying, screening, and choosing pertinent research articles for lightweight cryptography and IoT system authentication. A total of 1837 articles were first gathered from three main sources during the identification stage: IEEE Access (1661 articles), MDPI journals (128 articles), and other reputable journals (48

articles). To guarantee dataset consistency and relevance, duplicate and overlapping records were eliminated at this point. The identified publications were assessed throughout the screening and filtering phase using predetermined inclusion and exclusion criteria, including hardware implementation, IoT/WSN application, authentication procedures, and relevance to lightweight block ciphers. Consequently, 209 papers were selected for in-depth evaluation, whereas 1628 articles were eliminated for being irrelevant, redundant, or lacking technical depth. Full-text versions of the articles that made the short list were carefully examined throughout the eligibility stage to evaluate experimental validation, hardware performance reporting, and methodological rigor. 159 articles were eliminated after this thorough analysis due to inadequate technical contribution or incomplete evaluation. Ultimately, fifty excellent articles were judged qualified and chosen for the thorough literature review, which served as the foundation for the study's comparison analysis, findings, and discussion.

Fig. 1. Methodology adopted for Systematic review: PRISMA Flow

The inclusion and exclusion criteria used to guarantee the applicability, calibre, and technical accuracy of the systematic literature review on lightweight block ciphers and authentication methods for devices with limited resources are compiled in Table I. To capture recent and significant research, temporal and source-related limitations were first applied. To ensure alignment with current IoT security needs and advanced hardware platforms, only publications published between 2018 and 2026 were taken into consideration. Additionally, to preserve consistency, peer-review quality, and reproducibility, publications were limited to reputable journals, particularly IEEE and MDPI; conference papers and other non-journal sources were removed.

Second, to guarantee technical focus and clarity, linguistic and cryptography scope constraints were established. To enable consistent evaluation and interpretation, only publications written in English were included. From a cryptographic standpoint, the analysis only looked at hash or encryption primitives based on block ciphers, which are frequently employed in lightweight security solutions. The study did not include studies that focused on stream ciphers, asymmetric cryptography, or unrelated primitives. Lastly, to guarantee practical significance, limits at the technical and implementation levels were implemented. In accordance with widely recognized security standards for lightweight cryptography, only designs that supported a minimum block/key size of 32/64 bits or more were included. Furthermore, since the review's main goal was to assess the trade-offs between area, power, latency, and throughput in low-resource hardware contexts, it focused on hardware implementations on FPGA or ASIC platforms rather than just software-based solutions.

Table I

SELECTION and REJECTION criteria used in the systematic review

Criteria	Inclusion	Exclusion
Year of publication	After 2018	Before 2018
Article type	Only Journals (IEEE, MDPI)	Conference and other sources
Language	English	Non-English
Cryptographic Primitive	Block cipher and Hash function	Stream ciphers, asymmetric and others
Block/Key Size	32/64-bit and higher	Below 32/64-bit
Implementation	FPGA, ASIC	Software implementations

2.1 Recent findings on Lightweight block ciphers

The existing works of recent lightweight ciphers are discussed in this section. Mohd and Hayajneh [11] examine energy-efficient lightweight cipher structures for low-resource IoT gadgets and suggest an energy administration technique to counteract battery-exhaustion-based Denial-of-Service (DoS) assaults. They report optimal performance for block sizes between 48 and 96 bits and a 3.4% increase in energy per bit when extra round logic is added. Abed *et*

al. [12] finds that while pipelined executions accomplish up to 12x higher throughput with 31% lower energy use, scalar designs reduce resource utilization by 39% and power usage by 45% in their evaluation of SIMON cipher deployments. The two-round pipelined design is found to be the most environmentally friendly. Haider *et al.* [13] can maintain over 99% fault coverage while lowering hardware area expense by 23% and increasing throughput per slice by 14% by integrating an inexpensive self-test framework with PRESENT. Dahiphale *et al.* [14] describe FPGA adaptations of the ANU cipher employing 4-, 8-, 16-, and 32-bit data paths to compare the performance, area, and scalability of various FPGA platforms. Bharathi and Parvatham [15] present a hybrid Feistel–SPN-based LEA-SIoT cipher that outperforms AES by 10.49% in area and 48.37% in power by having a throughput of 7.989 Gbps and a power usage of 0.249 W. Enhanced PRINCE architectures are reported by Li *et al.* [16], with the unrolled structure achieving 5.34 Gbps speed and the low-cost design taking up only 137 slices. Bit-slicing GPU-based versions of PRESENT and GIFT with throughputs above 500 Gbps are demonstrated by Kim *et al.* [17]. A latency-optimized SIMECK FPGA architecture that can complete encryption and decryption in 16 clock cycles with a minimum power usage of 172 mW is presented by Alharbi *et al.* [18]. Zhang et al. [19] provides the GFRX cipher, which demonstrates resilience to differentiated assaults up to 19 rounds and linear assaults up to 13 rounds. While Youssef et al. [20] combine chaos-based number generation with Speck64/128 to improve security for IoT contexts.

A PRESENT-based hardware accelerator to support medical IoT devices is shown by Damodharan *et al.* [21], which use a low-latency 32-bit Datapath to achieve an 85.54% increase in throughput. An embedded PRESENT-256 framework that operates at 412.4 MHz and uses 192 mW corresponding to less than 2% of FPGA resources is implemented by Bharathi and Parvatham [22]. Employing an improved generalized Feistel network, Shah *et al.* [23] create a lightweight encryption that meets avalanche and randomness requirements in fewer rounds. Tran *et al.* [24] present a NIST-compliant ASCON hardware configuration that uses 2812 slices to achieve 8.806 Gbps throughput with 427 ns latency. The SLA cipher, which supports 80/128-bit keys with increased throughput and small hardware, is introduced by Ibrahim and Agbinya [25]. A stochastic lightweight encryption with over 60% avalanche features and 853.31 Kbps performance utilizing just 1510 bytes of memory is described by Aziz *et al.* [26]. Consolidated Ascon-128 and Ascon-128a FPGA versions working over 300 MHz with a power usage between 219 and 239 mW are evaluated by Alharbi *et al.* [27]. SPECK is the highest resource-effective of AES, SPECK, and ASCON on limited IoT devices, according to Radhakrishnan *et al.* [28]. Rana *et al.* [29] emphasize energy-conscious design trade-offs by providing accurate power estimations utilizing the Qoitech Otii Arc. Imdad *et al.* [30] use DNA-based procedures to boost PRESENT, resulting in a lower latency of 17 cycles per block, enhanced diffusion, and a throughput gain of 176.47 kb/s. LED cipher throughputs for 64-, 128-, and 256-bit keys are 3.869, 1.929, and 1.307 Gbps, respectively, according to Naik *et al.* [31]. A redesigned SPECK with enhanced key scheduling and statistical capabilities is proposed by Mohanapriya and Kumar [32]. Liu and Tang et al. [33] use threshold approaches to lower the secured uBlock slice area by 41.5%. Ahmed *et al.* [35] thoroughly examines lightweight AES structures, highlighting optimization patterns and unsettled security–efficiency trade-offs, whereas Anton *et al.* [34] present a hybrid SIMECK–TEA encryption with robust statistical randomization.

2.2 Recent findings on Authentication approaches

This section discusses contemporary authentication approaches that have been developed. To protect large-scale data-driven IoT devices, Atiewi *et al.* [36] provide a cloud-driven IoT structure that incorporates multifactor authentication and compact cryptographic encryption. The structure is assessed using metrics like processing time, encryption/decryption latency, and security effectiveness. Building on the SKINNY compact block cipher, Xiao *et al.* [37] present an RFID mutual authentication (MA) technique that is resistant to replay, tracing, and desynchronization while still being appropriate for inexpensive RFID tags. The initial threshold implementation of SAEAES is presented by Sugawara *et al.* [38], establishing compatibility with prior versions with an area expenditure of 18,288 gate equivalents (GE), where AES logic takes up almost 97% of the overall area. A versatile adoption of the Gimli authenticated encryption (AE) and hashing algorithm for RFID authentication is described by Khan *et al.* [39]. It achieves speeds of 740 Mbps and 420 Mbps in area- optimized structures and up to 3.08 Gbps and 1.43 Gbps in speed-focused approaches for hash and AE modes, accordingly. A practical RFID MA system utilizing XTEA in cipher

block chaining (CBC) mode is presented by Anusha *et al.* [40]. It operates at 263.762 MHz with a power use of 0.172 W and achieves an overall validation execution time of 11.555 µs. By integrating CBC-PRESENT and HMAC-PHOTON, Ngo *et al.* [41] suggest an area- and energy-efficient authentication framework that achieves gate counts of 5683 and 20,698 with low power use of 1.03 mW and 2.62 mW, respectively, with throughput measurements of 182.9 Mbps and 14.9 Mbps at 100 MHz, which leads to up to 75.28% power savings over traditional approaches.

Winarno *et al.* [42] construct a secure end-to-end MQTT protocol employing compact block cipher–based AE. Tiny JAMBU yields the most rapid efficiency, afterwards AES-128-GCM, GIFT-COFB, and Romulus-N1, according to experimental data. Light Secure Access Enhancement (Light-SAE), a compact key distribution and multi-hop authentication mechanism for WSNs, is introduced by Rosa *et al.* [43]. It shows quick authentication computation and favourable effectiveness in comparison to other techniques. Additionally, Anusha *et al.* [44] suggest compact RFID MA methods that use the XTEA and Hummingbird procedures in CBC mode. These methods need less than 2% of FPGA resources and have validation times of 11.6 µs and 1.34 µs, respectively. For RFID technologies, Bharathi and Peter [45] construct a PRESENT-256-based authentication mechanism that uses about 2% of slices, runs at 403.1 MHz, and uses 0.12 W of power. Al-Shatari *et al.* [46] provides a lightweight AE strategy that combines the PHOTON hashing algorithm with the LED block cipher, resulting in up to 46.04% reduced power usage and a 14% reduction in logic area when contrasted with individual systems. The Simple Hybrid Cipher (SHC-64), which requires just 949 LUTs and achieves an ultimate frequency of 515.995 MHz on an Artix-7 FPGA despite exhibiting resilience to known cryptanalytic assaults, is presented by Kumar *et al.* [47]. A mean execution time of 79.26 ms on Raspberry Pi systems is reported by Cagua *et al.* [48] in their analysis of ASCON effectiveness on IoT gadgets, enabling near-real-time encrypted interaction. An extremely compact MA mechanism with a mean efficiency gain of 78.51% over current approaches and an overall operation time of 0.031 ms is proposed by Alhasan *et al.* [49]. Lastly, the URASP and KUAJB protocols are thoroughly examined by Hosseinzadeh *et al.* [50], who identify weaknesses to private disclosure assaults and suggest improving the protocol using compact encryption primitives.

3. RESULTS AND DISCUSSION

The performance outcomes of the current Lightweight block ciphers and authentication techniques are thoroughly discussed in this section. The investigation focuses on the way area usage, operational frequency, power usage, latency, throughput, and overall effectiveness are affected by architectural decisions, target platforms, and security goals. For lightweight cryptographic implementations in limited contexts like IoT nodes, RFID tags, and integrated edge gadgets, these characteristics are essential. Several types of lightweight block cipher algorithms implemented on various FPGA systems are evaluated in Table II.

Initial lightweight architectures that emphasize simple and tiny logic, like SIMON [12] and PRESENT [13], have comparatively low power usage and area usage. But these advantages come at the expense of lower throughput, especially in SIMON, which only offers 280.2 Mbps throughput and works at a rather low frequency of 66.2 MHz. This suggests that low hardware cost rather than efficient encryption was the main goal of first-generation lightweight ciphers. Performance-oriented structures are clearly becoming more prevalent in the following designs. For example, ANU [14] uses strong parallelism and a larger Datapath to dramatically boost throughput to 1432.5 Mbps. This increases encryption speed, but it also results in higher power usage (573.35 mW) and LUT usage, underscoring the intrinsic trade-off between energy economy and throughput. Like this, SIoT-LEA [15] uses pipelined and unrolled designs to deliver extraordinarily high capacity (7982 Mbps) with single-cycle latency. This architecture is appealing for high-speed use cases; however, it is not suitable for ultra-constrained systems due to its enormous LUT and slice count.

A more balanced solution is provided by PRINCE [16], which combines modest area utilization, fast throughput (4436.16 Mbps), and minimal latency (2 clock cycles). PRINCE is appropriate for real-time automation and latency-critical IoT gateways because of this balance. SIMECK [18], on the other hand, uses just 50 slices and 164 LUTs to minimize area and power usage. These features make it ideal for RFID and sensors where energy savings and portability are crucial, even though its throughput (24.39 Mbps) is much lower. More optimizations can be seen in

recent hybrid and standardized designs. To show that security adaptability affects latency and performance, SPCNG [20] and several PRESENT versions [21], [22] investigate various key sizes and pipeline depths. Notably, PRESENT-256 [22] illustrates the expense of larger key sizes by achieving enhanced security with controllable power usage (192 mW) but incurring increased latency (64 cycles). ASCON-based solutions [24], [27], which adhere to NIST lightweight encryption requirements, provide continuously excellent performance (up to 13.3 Gbps) with manageable area overhead, confirming their appropriateness for IoT deployments that are future-proof. Efficiency is further emphasized by LED-based systems [31] and M-SPECK [32], which demonstrate that meticulous round reduction and Datapath utilization can greatly improve throughput-per-area ratios. Overall, Table 2 shows that architectural choices like pipelining, unrolling, and key scheduling have a significant impact on the performance of lightweight block ciphers. While ultra-compact designs promote low power usage at the expense of speed, throughput-optimized systems frequently sacrifice power and area efficiency.

The increasing need for comprehensive security features beyond confidentiality is shown in Table III, which focuses on authentication and AE techniques applied across FPGA and ASIC architectures. Gimli-based authentication [39] has comparatively high latency (262 cycles) and moderate space needs and throughput (428.68 Mbps), indicating that it is appropriate for situations where resilience and permutation-based assurance are more important than real-time efficiency.

Table II.

Performance comparison of the Existing lightweight ciphers on Various FPGAs

Designs	Year	Cipher name	Data/Key	Slices	LUTs	FFs	Freq (MHz)	Power (mW)	Latency (CC)	Throughput (Mbps)	Efficiency (Mbps/Slice)	FPGA
Ref [12]	2020	SIMON	32/64	NA	210	NA	66.2	168	32	280.2	1.33	Altera
Ref [13]	2019	PRESENT	64/80	97	215	154	695	NA	32	381.52	1.71	Kintex-7
Ref [14]	2020	ANU	64/128	103	270	199	559.56	573.35	25	1432.5	3.36	Virtex-5
Ref [15]	2020	SIoT-LEA	64/64	211	1578	200	249.46	2.49	1	7982	37.82	Artix-7
Ref [16]	2021	PRINCE	64/128	451	1279	69	138.63	NA	2	4436.16	9.84	Virtex-6
REF [18]	2023	SIMECK	32/64	50	164	89	388.52	189.77	16	24.39	0.487	Artix-7
Ref [20]	2023	SPCNG	64/128	99	1079	67	51.25	NA	64	3280	3.12	Pynq-Z2
Ref [21]	2023	PRESENT	64/80	59	185	169	703	275.4	65	692.85	0.118	Zynq-Z2
Ref [22]	2022	PRESENT	64/256	711	617	471	413	192	64	413	0.58	Artix-7
Ref [24]	2023	ASCON-128A	128/128	282	6536	NA	104	NA	128	13312	2.306	Virtex-7
Ref [27]	2024	ASCON-128A	128/128	348	1632	912	335	239	47	400	1.14	Virtex-7

Ref [31]	2024	LED	64/64	133	273	133	409	NA	8	3265	24.55	Artix-7
Ref [31]	2024	LED	64/128	133	275	133	407	NA	16	1629	12.25	Artix-7
Ref [32]	2025	M-SPECK	32/64	NA	240	NA	154	175	32	154	0.64	Artix-7
Ref [33]	2025	uBlock	128/128	289	773	707	324.93	NA	64	650	2.24	Kintex-7

Table III.

Performance comparison of the existing Authentication-based approaches on Various FPGAs and ASICs

Parameters	REF [39]	Ref [40]	Ref [41]	Ref [41]	Ref [44]	Ref [45]	Ref [45]	Ref [45]	Ref [46]	Ref [47]
Year	2021	2021	2022	2022	2023	2023	2023	2023	2023	2024
Cipher Type	Gimili-Hash	XTEA	PRESENT	PHOTON-Hash	HB	PRESENT	PRESENT	PRESENT	LED/ PHOTON	SEC
Data/Key	128/128	64/128	64/128	128/128	16/256	64/80	64/128	64/256	100	64/128
Slices OR (GE)	NA	1604	5680	17359	1645	754`	945	1457	1030	339
LUTs	1710	2307	NA	NA	1998	1086	1276	1783	NA	949
Freq (MHz)	408.59	263.77	100	100	349	404	404	404	140.39	515.9
Power (mW)	NA	172	1.03	2.62	155	107	114	120	99.3	2.361
Latency (CC)	262	128	70	860	12	32	32	32	140	28
Throughput (Mbps)	428.68	132	188.2	14.9	503	808	808	808	100.71	2362
Efficiency (Kbps/Slice)	250	8.2	3.3	0.09	350	1071	856	555	97.7	6.96
Execution Time (µs)	1419	11.55	NA	NA	1.34	1.285	1.285	1.285	NA	28.56
Platform	Sparta n-6	Artix-7	ASIC (65nm)	ASIC (65nm)	Artix-7	Artix-7	Artix-7	Artix-7	Cyclone-II	Artix-7

For RFID authentication methods that need quick challenge-response processes, XTEA-based authentication [40] offers a favourable balance between execution time (11.55 µs), power usage (172 mW), and area. Power efficiency is further enhanced by PRESENT-based authentication systems [41], [45], particularly in ASIC versions where power lowers to as low as 1.03 mW. This demonstrates the benefit of ASIC platforms for battery-powered devices, even though they come at the expense of less flexibility after manufacturing.

Hash-based authentication methods that prioritize security

effectiveness and compactness include PHOTON [41]. Although these designs have lesser throughput and higher

latency (up to 860 cycles), they offer robust defense against cryptographic assaults, which makes them appropriate for data integrity validation and safe boot. One notable example of how hybrid stream-block cipher designs may effectively accommodate low-latency authentication is Hummingbird (HB) [44], which achieves high throughput (503 Mbps) and a short execution time (1.34 μs).

By sharing internal parts across encryption and authentication modules, integrative authenticated encryption techniques, such LED/PHOTON [46], provide significant savings in logic space and power usage. This integration results in decreased hardware duplication and increases overall efficiency. With comparatively little LUT utilization, the Simple Hybrid Cipher (SEC) [47] delivers one of the highest throughputs (2362 Mbps), demonstrating that well-coordinated encryption and authentication primitives may surpass independent approaches in hardware systems with limited resources.

A basic trade-off between complete security and perfect encryption performance is revealed by comparing Tables II and III. Because their control logic is simpler, lightweight block ciphers typically achieve faster throughput and lower delay, whereas authentication-based methods require extra computational expense to guarantee authenticity and integrity. While ASIC-based solutions excel in extremely low power usage and lightweight, FPGA-based versions prioritize scalability and great performance. These findings suggest that design choices should be based on the application's demands. While PRESENT, SIMECK, and XTEA-based authentication techniques are more appropriate for severely limited IoT and RFID contexts, high-throughput ciphers like ASCON and SIoT-LEA are appropriate for edge gateways and rapid connectivity nodes. In the end, the thorough analysis demonstrates that the most viable path for safe, energy-efficient next-generation embedded systems involves incorporating lightweight encryption and authentication designs.

3.1 Research Gaps

Although lightweight block ciphers and authentication methods for FPGA-based platforms have advanced significantly, the literature and comparative analysis examined show that there are still several unsolved research issues.

- A major limitation is the absence of thorough optimization across several hardware metrics. Most of the current research concentrates on a single design goal, such as lowering power usage, increasing throughput, or shrinking hardware area, without simultaneously optimizing latency, hardware efficiency, and security robustness. The comparison results show that whereas area-efficient implementations typically have higher latency and lower throughput, systems that achieve high throughput and low latency frequently incur significant LUT and slice overheads. Their use in heterogeneous IoT and WSN contexts, where several performance restrictions must be met at once, is limited by this fragmented optimization.
- The limited integration of lightweight encryption with authentication systems is another significant research gap. Although numerous authentication-based techniques have been presented, they often contribute increased computational complexity, delay, and hardware overhead compared to independent lightweight block ciphers. Many current cipher implementations do not inherently enable authentication or data integrity, hence necessitating extra cryptographic units that increase resource utilization and energy usage. For contemporary IoT applications, which increasingly require small, secure, and energy-efficient end-to-end interaction solutions, this division between encryption and authentication is insufficient.
- The reviewed literature also emphasizes that present-day cryptography designs are not flexible or scalable. Most implementations are designed with fixed block sizes, key lengths, and security parameters, making them

unsuitable for dynamic IoT and edge-computing scenarios where computational resources, energy availability, and security needs regularly fluctuate.

3.2 Future Scope

The creation of unified lightweight cryptographic systems that smoothly combine authentication and encryption into a single hardware framework should be the main emphasis of future research. Instead of evaluating these variables separately, such systems should strive to collectively maximize hardware space, power usage, latency, throughput, and security. By striking this balance, lightweight cryptographic systems will be able to better meet the demanding requirements of next-generation RFID, IoT, and WSN systems.

- The development of adaptive and reconfigurable FPGA-based cryptography systems that may dynamically modify hardware resources and security levels in response to application needs is another interesting avenue. Approaches such as partial dynamic reconfiguration, adaptive datapath topologies, customizable key sizes, and clock/voltage scaling can enable flexible trade-offs between security, performance, and energy consumption. Without the need for different cryptographic implementations, these adaptive methods will enable a single hardware design to accommodate a variety of IoT applications.
- The inclusion of implementation-level security functions, such as protection against side-channel attacks, fault injection attacks, and other physical threats, should also be emphasized in future research. Integrating lightweight countermeasures with little hardware overhead remains a key research topic for practical deployments. Furthermore, the adoption of NIST-standard lightweight cryptographic techniques, authenticated encryption with associated data (AEAD) schemes, and hybrid encryption–authentication frameworks will further strengthen the security of resource-constrained systems while maintaining acceptable hardware efficiency.
- Finally, there is an urgent need to establish standardized benchmarking and assessment procedures for lightweight cryptographic implementations. Future research should use standard FPGA and ASIC platforms, uniform performance metrics, and consistent assessment criteria spanning hardware utilization, throughput, latency, power usage, energy efficiency, security resilience, and resistance to physical attacks. Standardized assessment frameworks will make it possible to compare competing techniques fairly, make research more replicable, and hasten the practical deployment of lightweight cryptography in new edge-computing and IoT applications.

4. CONCLUSION

Modern lightweight block ciphers and authentication-based cryptographic methods aimed at devices with limited resources were thoroughly examined in this review. High-quality journal articles were examined utilizing a systematic PRISMA-based selection method, with a focus on FPGA and ASIC hardware implementations. The comparison findings show that, depending on architectural decisions like pipelining, Datapath width, and unrolling, lightweight block ciphers display various trade-offs between area, throughput, latency, and power. To minimize costs while preserving security, integrated encryption–authentication primitives are becoming more and more popular in authentication-oriented designs, such as mutual authentication protocols and AEAD. Nevertheless, the analysis shows significant shortcomings in unified lightweight security structures, side-channel-aware design, and consistent benchmarks. All things considered, the study offers researchers and designers a comprehensive technical resource that sheds light on contemporary design trends, performance constraints, and unresolved issues. Additionally, it lays the framework for future studies into lightweight cryptographic designs that are secure, scalable, and energy-efficient for embedded systems and the next generation of IoT.

Chaitra P is currently working as Assistant Professor in the department of Computer Science and Engineering at Atria Institute of Technology, Bangalore. She received her M tech degree from VTU (2016) in VLSI design and Embedded system and BE from VTU (2014) in Electronics and Communication System. She carries a PG Certification degree program in CPS (Cyber Physical System from IIIT Dharwad. She is an active member of IEEE RAS society and ISTE. She has published papers on IoT, Machine Learning and Artificial Intelligence in IEEE Conferences and

Scopus index. Her Research interests include Cryptography, IoT, Machine learning, Embedded System and Network security. She can be contacted at: chaitrap31@gmail.com.

Shobha I. Hugar is currently working as an Professor and HOD in the Department of Electronics and Communication Engineering at Sapthagiri College of Engineering, Bangalore, India. She received Ph.D. degree in RF and Microwave Passive Devices from Visvevsaraya Technological University, Belagavi, India in 2022. She received B.E. and M.Tech. degrees in Electronics and Communication Engineering and VLSI Design and Embedded Systems from Karnataka University, Dharwad, Visvevsaraya Technological University, Belagavi, India, in 2000 and 2008, respectively. She is member of IEEE Microwave Theory and Technique Society (MTT-S) and Institution of Electronics and Telecommunication Engineers (IETE). Her current research include microwave and millimeter wave components, antenna , CMOS RF circuit design and low power VLSI. She published many research papers in Microwave & Optical Technology letters(Wiley), IETE Journal of Research (Taylor & Francis), Procedia (Elsevier), Radioengineering and Progress In Electromagnetic Research (PIER) journals. She can be contacted at: shobha_hugar@yahoo.co.in.

REFERENCES

1. V. A. Thakor, M. A. Razzaque and M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," in IEEE Access, vol. 9, pp. 28177-28193, 2021, doi: 10.1109/ACCESS.2021.3052867.
2. M. El-hajj, H. Mousawi, and A. Fadlallah, “Analysis of lightweight cryptographic algorithms on IoT hardware platform,” *Future Internet*, vol. 15, no. 2, p. 54, 2023, doi: 10.3390/fi15020054.
3. S. M. Al-Nofaie, S. Sharaf, and R. Molla, “Design trends and comparative analysis of lightweight block ciphers for IoTs,” *Appl. Sci. (Basel)*, vol. 15, no. 14, p. 7740, 2025, doi: 10.3390/app15147740.
4. H. Madushan, I. Salam, and J. Alawatugoda, “A review of the NIST lightweight cryptography finalists and their fault analyses,” *Electronics (Basel)*, vol. 11, no. 24, p. 4199, 2022, doi: 10.3390/electronics11244199.
5. I. Cetintav and M. Tahir Sandikkaya, "A Review of Lightweight IoT Authentication Protocols From the Perspective of Security Requirements, Computation, Communication, and Hardware Costs," in IEEE Access, vol. 13, pp. 37703-37723, 2025, doi: 10.1109/ACCESS.2025.3546147.
6. T. Nandy et al., "Review on Security of Internet of Things Authentication Mechanism," in IEEE Access, vol. 7, pp. 151054-151089, 2019, doi: 10.1109/ACCESS.2019.2947723.
7. J. S. Yalli et al., "A Systematic Review for Evaluating IoT Security: A Focus on Authentication, Protocols and Enabling Technologies," in IEEE Internet of Things Journal, vol. 12, no. 12, pp. 18908-18928, 15 June15, 2025, doi: 10.1109/JIOT.2025.3545737.
8. M. Abbas Fadhil Al-Husainy, B. Al-Shargabi, and O. Sabri, “Super Encryption Standard (SES): A key-dependent block cipher for image encryption,” *Information (Basel)*, vol. 17, no. 1, p. 2, 2025, doi: 10.3390/info17010002.
9. S. Alsaraireh, A. Ahmad, and Y. AbuHour, “New step in lightweight medical image encryption and authenticity,” *Mathematics*, vol. 13, no. 11, p. 1799, 2025, doi: 10.3390/math13111799.
10. O. Sabri, B. Al-Shargabi, A. Abuarqoub, and T. A. Hakami, “A lightweight encryption method for IoT-based healthcare applications: A review and future prospects,” *IoT*, vol. 6, no. 2, p. 23, 2025, doi: 10.3390/iot6020023.
11. B. J. Mohd and T. Hayajneh, "Lightweight Block Ciphers for IoT: Energy Optimization and Survivability Techniques," in IEEE Access, vol. 6, pp. 35966-35978, 2018, doi: 10.1109/ACCESS.2018.2848586.
12. S. Abed, R. Jaffal, B. J. Mohd, and M. Alshayeji, “FPGA modeling and optimization of a SIMON lightweight block cipher,” *Sensors (Basel)*, vol. 19, no. 4, p. 913, 2019, doi: 10.3390/s19040913.
13. Z. Haider, K. Javeed, M. Song and X. Wang, "A Low-Cost Self-Test Architecture Integrated With PRESENT Cipher Core," in IEEE Access, vol. 7, pp. 46045-46058, 2019, doi: 10.1109/ACCESS.2019.2907717.
14. V. Dahiphale, G. Bansod, A. Zambare and N. Pisharoty, "Design and Implementation of Various Datapath Architectures for the ANU Lightweight Cipher on an FPGA," in Frontiers of Information Technology & Electronic Engineering, vol. 21, no. 4, pp. 615-628, April 2020, doi: 10.1631/FITEE.1800681.
15. Bharathi and N. Parvatham, “LEA-SIoT: Hardware architecture of lightweight encryption algorithm for secure IoT on FPGA platform,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 1, 2020, doi: 10.14569/ijacsa.2020.0110189.
16. L. Li, J. Feng, B. Liu, Y. Guo and Q. Li, "Implementation of PRINCE with Resource-Efficient Structures based on FPGAs," in Frontiers of Information Technology & Electronic Engineering, vol. 22, no. 11, pp. 1505-1516, November 2021, doi: 10.1631/FITEE.2000688.
17. H. Kim, S. Eum, W.-K. Lee, S. Lee, and H. Seo, “Secure and robust Internet of Things with high-speed implementation of PRESENT and GIFT block ciphers on GPU,” *Appl. Sci. (Basel)*, vol. 12, no. 20, p. 10192, 2022, doi: 10.3390/app122010192.
18. A. R. Alharbi, H. Tariq, A. Aljaedi, and A. Aljuhni, “Latency-aware accelerator of SIMECK lightweight block cipher,” *Appl. Sci. (Basel)*, vol. 13, no. 1, p. 161, 2022, doi: 10.3390/app13010161.
19. X. Zhang, S. Tang, T. Li, X. Li, and C. Wang, “GFRX: A new lightweight block cipher for resource-constrained IoT nodes,” *Electronics (Basel)*, vol. 12, no. 2, p. 405, 2023, doi: 10.3390/electronics12020405.

20. W. E. H. Youssef et al., "A Secure Chaos-Based Lightweight Cryptosystem for the Internet of Things," in IEEE Access, vol. 11, pp. 123279-123294, 2023, doi: 10.1109/ACCESS.2023.3326476.
21. J. Damodharan, E. R. Susai Michael, and N. Shaikh-Husin, “High throughput PRESENT cipher hardware architecture for the medical IoT applications,” *Cryptography*, vol. 7, no. 1, p. 6, 2023, doi: 10.3390/cryptography7010006.
22. R. Bharathi and N. Parvatham, “Light-weight present block cipher model for IoT security on FPGA,” *Intell. Autom. Soft Comput.*, vol. 33, no. 1, pp. 35–49, 2022, doi: 10.32604/iasc.2022.020681.
23. I. N. Mohammad Shah, E. S. Ismail, F. Samat, and N. Nek Abd Rahman, “Modified generalized Feistel network block cipher for the Internet of Things,” *Symmetry (Basel)*, vol. 15, no. 4, p. 900, 2023, doi: 10.3390/sym15040900.
24. S. -N. Tran, V. -T. Hoang and D. -H. Bui, "A Hardware Architecture of NIST Lightweight Cryptography Applied in IPSec to Secure High-Throughput Low-Latency IoT Networks," in IEEE Access, vol. 11, pp. 89240-89248, 2023, doi: 10.1109/ACCESS.2023.3306420.
25. N. Ibrahim and J. Agbinya, “Design of a lightweight cryptographic scheme for resource-constrained internet of things devices,” *Appl. Sci. (Basel)*, vol. 13, no. 7, p. 4398, 2023, doi: 10.3390/app13074398.
26. S. Aziz *et al.*, “Next-generation block ciphers: Achieving superior memory efficiency and cryptographic robustness for IoT devices,” *Cryptography*, vol. 8, no. 4, p. 47, 2024, doi: 10.3390/cryptography8040047.
27. A. R. Alharbi, A. Aljaedi, A. Aljuhni, M. K. Alghuson, H. Aldawood and S. S. Jamal, "Evaluating Ascon Hardware on 7-Series FPGA Devices," in IEEE Access, vol. 12, pp. 149076-149089, 2024, doi: 10.1109/ACCESS.2024.3471694.
28. I. Radhakrishnan, S. Jadon, and P. B. Honnavalli, “Efficiency and security evaluation of lightweight cryptographic algorithms for resource-constrained IoT devices,” *Sensors (Basel)*, vol. 24, no. 12, p. 4008, 2024, doi: 10.3390/s24124008.
29. M. Rana, Q. Mamun, and R. Islam, “Balancing security and efficiency: A power consumption analysis of a lightweight block cipher,” *Electronics (Basel)*, vol. 13, no. 21, p. 4325, 2024, doi: 10.3390/electronics13214325.
30. M. Imdad, A. Fazil, S. N. B. Ramli, J. Ryu, H. B. Mahdin, and Z. Manzoor, “DNA-PRESENT: An improved security and low-latency, lightweight cryptographic solution for IoT,” *Sensors (Basel)*, vol. 24, no. 24, p. 7900, 2024, doi: 10.3390/s24247900.
31. M. S. Naik, D. K. Sreekantha, and K. V. S. S. S. S. Sairam, “An efficient low-latency and high throughput LED cipher architecture for IoT security on a hardware platform,” *SN Comput. Sci.*, vol. 5, no. 7, 2024, doi: 10.1007/s42979-024-03275-5.
32. R. Mohanapriya and V. Nithish Kumar, "Modified SPECK (M-SPECK) Lightweight Cipher Architecture for Resource-Constrained Applications," in IEEE Access, vol. 13, pp. 88993-89002, 2025, doi: 10.1109/ACCESS.2025.3570727.
33. B. Liu and M. Tang, "A Very Compact and a Threshold Implementation of uBlock for Internet of Things," in Tsinghua Science and Technology, vol. 30, no. 5, pp. 2270-2283, October 2025, doi: 10.26599/TST.2024.9010257.
34. A.-A. Anton, P. Csereoka, E.-A. Capota, and R.-D. Cioargă, “SIMECK-T: An ultra-lightweight encryption scheme for resource-constrained devices,” *Appl. Sci. (Basel)*, vol. 15, no. 3, p. 1279, 2025, doi: 10.3390/app15031279.
35. S. Ahmed et al., "Lightweight AES Design for IoT Applications: Optimizations in FPGA and ASIC With DFA Countermeasure Strategies," in IEEE Access, vol. 13, pp. 22489-22509, 2025, doi: 10.1109/ACCESS.2025.3533611. keywords: {Internet of Things;Field programmable gate
36. S. Atiewi et al., "Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography," in IEEE Access, vol. 8, pp. 113498-113511, 2020, doi: 10.1109/ACCESS.2020.3002815.
37. L. Xiao, H. Xu, F. Zhu, R. Wang, and P. Li, “SKINNY-based RFID lightweight authentication protocol,” *Sensors (Basel)*, vol. 20, no. 5, p. 1366, 2020, doi: 10.3390/s20051366.
38. T. Sugawara, “Hardware performance evaluation of authenticated encryption SAEAES with threshold implementation,” *Cryptography*, vol. 4, no. 3, p. 23, 2020, doi: 10.3390/cryptography4030023.
39. S. Khan, W. -K. Lee and S. O. Hwang, "A Flexible Gimli Hardware Implementation in FPGA and Its Application to RFID Authentication Protocols," in IEEE Access, vol. 9, pp. 105327-105340, 2021, doi: 10.1109/ACCESS.2021.3100104.
40. R. Anusha and V. V. D. Shastrimath, "RFID-MA XTEA: Cost-Effective RFID Mutual Authentication Design Using XTEA Security on FPGA Platform," *Intl Journal of Electronics and Telecommunications,* vol. 67, no. 4, pp. 623–629, 2021, doi: 10.24425/IJET.2021.137855.
41. T. Ngo, J. K. Eshraghian, and J.-P. Hong, “An area-optimized and power-efficient CBC-PRESENT and HMAC-PHOTON,” *Electronics (Basel)*, vol. 11, no. 15, p. 2380, 2022, doi: 10.3390/electronics11152380.
42. A. Winarno and R. F. Sari, “A novel Secure End-to-End IoT communication scheme using lightweight cryptography based on Block Cipher,” *Appl. Sci. (Basel)*, vol. 12, no. 17, p. 8817, 2022, doi: 10.3390/app12178817.
43. P. Rosa, A. Souto and J. Cecílio, "Light-SAE: A Lightweight Authentication Protocol for Large-Scale IoT Environments Made With Constrained Devices," in IEEE Transactions on Network and Service Management, vol. 20, no. 3, pp. 2428-2441, Sept. 2023, doi: 10.1109/TNSM.2023.3275011.
44. R, R. R. P and P. R. N, "Secured Authentication of RFID Devices Using Lightweight Block Ciphers on FPGA Platforms," in IEEE Access, vol. 11, pp. 107472-107479, 2023, doi: 10.1109/ACCESS.2023.3320277.
45. B. Ramachandra and S. E. Peter, "Secured authentication of radio-frequency identification system using PRESENT block cipher," *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 13, no. 5, p. 5462, 2023, doi: 10.11591/ijece.v13i5.pp5462-5471.

46. M. Al-Shatari, F. A. Hussin, A. A. Aziz, T. A. E. Eisa, X.-T. Tran, and M. E. E. Dalam, “IoT edge device security: An efficient lightweight authenticated encryption scheme based on LED and PHOTON,” *Appl. Sci. (Basel)*, vol. 13, no. 18, p. 10345, 2023, doi: 10.3390/app131810345.
47. S. Kumar et al., "SHC: 8-bit Compact and Efficient S-Box Structure for Lightweight Cryptography," in IEEE Access, vol. 12, pp. 39430-39449, 2024, doi: 10.1109/ACCESS.2024.3372388.
48. Cagua, V. Gauthier-Umaña and C. Lozano-Garzon, "Implementation and Performance of Lightweight Authentication Encryption ASCON on IoT Devices," in IEEE Access, vol. 13, pp. 16671-16682, 2025, doi: 10.1109/ACCESS.2025.3529757.
49. A. Q. A. Alhasan, M. F. Rohani and M. S. Abu-Ali, "Ultra-Lightweight Mutual Authentication Protocol to Prevent Replay Attacks for Low-Cost RFID Tags," in IEEE Access, vol. 12, pp. 50925-50934, 2024, doi: 10.1109/ACCESS.2024.3386100.
50. M. Hosseinzadeh et al., "An Enhanced Authentication Protocol Suitable for Constrained RFID Systems," in IEEE Access, vol. 12, pp. 61610-61628, 2024, doi: 10.1109/ACCESS.2024.3364690.