Systematic Review of Lightweight Cryptographic Algorithms for IoT Security: Advances and Trends

Shilpa Shetty A [1], Sudeepa K B [2], Chaithra K M [3], Ananth Prabhu G [4]
[1] Research Scholar, NMAM Institute of Technology, Nitte (Deemed to be University), India | AJ Institute of Engineering and Technology, affiliated to VTU Belagavi, India
[2] Department of Computer Science and Engineering, NMAM Institute of Technology, Nitte (Deemed to be University), India
[3] Special Officer, Visvesvaraya Technological University, Belagavi, India
[4] Department of Computer Science and Engineering, Sahyadri College of Engineering and Management, Mangalore, India

ARTICLE INFORMATION

Article History:

Received 09 August 2025
Revised 26 September 2025
Accepted 12 November 2025

Keywords:

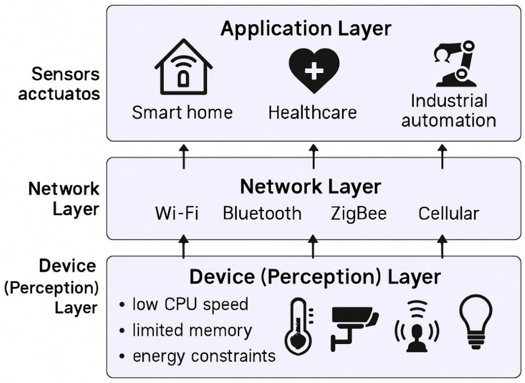
NIST LWC Standard;
Side-channel Resistance:
Resource-constrained Devices;
Lightweight Cryptography;
Post-Quantum

Corresponding Author:

Sudeepa K B,
Department of Computer Science and Engineering, NMAMIT, Nitte (Deemed to be University),
Nitte, India.
Email: sudeepa@nitte.edu.in

This work is open access under a Creative Commons Attribution-Share Alike 4.0

ABSTRACT



The proliferation of the Internet of Things (IoT) has fundamentally transformed modern infrastructure, but has also intensified security risks due to device resource constraints and interconnected environments. This systematic review synthesizes research on lightweight cryptographic algorithms for IoT security, focusing on studies published from 2019 to 2025. Relevant articles were identified through comprehensive searches of IEEE Xplore, ScienceDirect, Springer, and ACM Digital Library using Boolean strings that targeted terms including "lightweight cryptography," "IoT security," "side-channel resistance," and "NIST LWC Standard." Only peer-reviewed works in English addressing cryptographic primitives suitable for constrained IoT platforms were included; gray literature and studies without benchmarking on IoT-class hardware were excluded. Selection adhered to PRISMA guidelines to reduce selection bias. This review maps algorithmic taxonomies, highlights advances such as ASCON (NIST LWC 2025), side-channel and post-quantum resistance, and discusses real-world hardware-software trade-offs. Limitations arise from database scope, language constraints, and potential exclusion of emerging industry preprints. The analysis identifies persistent gaps—side-channel mitigations, context-aware security, and privacy—with guidance for future research. Overall, the findings clarify current capabilities and boundaries, supporting the development of scalable, energy-efficient, and robust cryptographic frameworks for secure IoT deployments within documented methodological limits.

Document Citation:

S. S. A, S. K B, and C. K M, Ananth Prabhu G, "Systematic Review of Lightweight Cryptographic Algorithms for IoT Security: Advances and Trends," *Buletin Ilmiah Sarjana Teknik Elektro*, vol. 7, no. 4, pp. 789-806, 2025, DOI: 10.12928/biste.v7i4.14440.

1. INTRODUCTION

The rapid expansion of the Internet of Things (IoT) is reshaping sectors from healthcare and industrial control to smart cities, yet the resulting proliferation of constrained endpoints—limited in processing, memory, energy, and cost—imposes stringent security requirements that conventional cryptography often cannot meet efficiently. Lightweight cryptography addresses this need by preserving confidentiality, integrity, and authentication with reduced computational, memory, and energy overheads tailored to embedded microcontrollers and ultra-low-power devices [1]. Lightweight primitives include block ciphers, stream ciphers, hash functions, and message authentication codes, with designs emphasizing efficient operations (for example, ARX, compact S-boxes, and permutation-based sponges) and careful implementation to balance security and performance on constrained platforms. The field has advanced with standardization milestones, including NIST's 2023 selection of the ASCON family for lightweight authenticated encryption and hashing, providing vetted, interoperable options for constrained environments [2]-[4].

Although multiple surveys exist, gaps remain in integrating the latest standardized solutions, evaluating post-quantum adaptations suited to edge and gateway roles, and establishing reproducible, platform-aware evaluation frameworks. This review systematically covers recent literature with criteria aligned to IoT deployment—cycles per byte, memory footprint, energy behaviour, and hardware area considerations-spanning sensors, embedded microcontrollers, and gateways. The objectives are to: classify and quantitatively compare lightweight algorithms tailored to IoT security; analyze hardware–software trade-offs under practical threat models, including side-channel attacks; highlight advances in standardization, post-quantum directions, and AI/ML-assisted optimization; and identify open challenges in side-channel resilience, privacy preservation, and adaptive, context-aware security. The next section links lightweight design tenets to IoT's device, network, and application layers, establishing how architectural constraints shape algorithm and parameter choices used throughout the taxonomy and comparative analysis that follow [5]-[8].

The key objectives of this review are to:

- Provide an in-depth classification and quantitative comparison of lightweight cryptographic algorithms tailored for IoT security;
- Analyze trade-offs in hardware and software implementations, considering practical threat models including side-channel attacks;
- Highlight advances in standardization, post-quantum cryptography, and AI/ML-based cryptographic optimizations;
- Identify remaining challenges related to side-channel resistance, privacy preservation, and adaptive security solutions responsive to IoT context variability.

By establishing a transparent scope and methodology, this work aims to provide a reproducible and actionable resource to researchers and practitioners securing the rapidly evolving IoT ecosystem.

2. REVIEW METHODOLOGY

2.1. Literature Search Strategy

This systematic review was conducted adhering to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure transparency and reproducibility [9]. A comprehensive search for relevant peer-reviewed articles published from January 2019 to July 2025 was performed across four foremost electronic databases: IEEE Xplore, ScienceDirect, SpringerLink, and the ACM Digital Library. The search employed a combination of Boolean keywords and phrases related to lightweight cryptography and IoT, including but not limited to: "lightweight cryptography," "lightweight encryption," "Internet of Things," "resource-constrained devices," "side-channel resistance," and "post-quantum cryptography." Inclusion was restricted to English-language articles published in journals or reputable conferences.

2.2 Screening and Selection Process

The initial database queries yielded 723 records. After removing 23 duplicates, 700 unique records underwent title and abstract screening to exclude studies irrelevant to lightweight cryptographic algorithms or IoT security applications. This screening reduced the pool to 245 articles. Subsequently, full-texts of these 245 papers were assessed against the following inclusion criteria:

- Articles must present original research focused on lightweight cryptographic algorithms applicable to resource-constrained IoT devices.
- Inclusion of quantitative benchmarking data such as hardware gate equivalents, memory utilization, computational cycles, or energy consumption.
- Utilization of standardized or real-world hardware/software platforms for performance assessment.

- Exclusion criteria comprised:
- Non-English publications and grey literature such as technical reports and white papers.
- Reviews lacking original data or benchmarking.
- Articles outside the defined time frame (pre-2019 or post-July 2025).

Following full-text evaluation, 78 articles satisfied the criteria and were included in the qualitative and quantitative analysis.

2.2. Data Extraction and Synthesis

Data extraction focused on capturing comprehensive information regarding algorithm taxonomy, performance metrics (cycles per byte, ROM/RAM usage, energy consumption), implementation methodology (hardware versus software), and security assessments, particularly resistance to side-channel and post-quantum attacks. The synthesis integrated both qualitative insights and quantitative performance comparisons to generate a holistic evaluation and trends.

2.3. PRISMA Flow Diagram Summary

The process of filtering the literature for this systematic review is summarized as follows and is visually represented in Figure 1. Initially, 723 records were identified through database searching. After removing 23 duplicate records, 700 unique records proceeded to title and abstract screening. Based on relevance criteria, 455 records were excluded at this stage. The remaining 245 full-text articles were then assessed for eligibility, leading to the exclusion of 167 articles due to reasons such as lack of original data, insufficient benchmarking, or irrelevance to lightweight cryptographic algorithms for IoT. Ultimately, 78 studies met all inclusion criteria and were incorporated into the qualitative synthesis. The systematic process by which relevant studies were identified, screened, assessed, and selected for inclusion in this review is illustrated in the Figure 1.

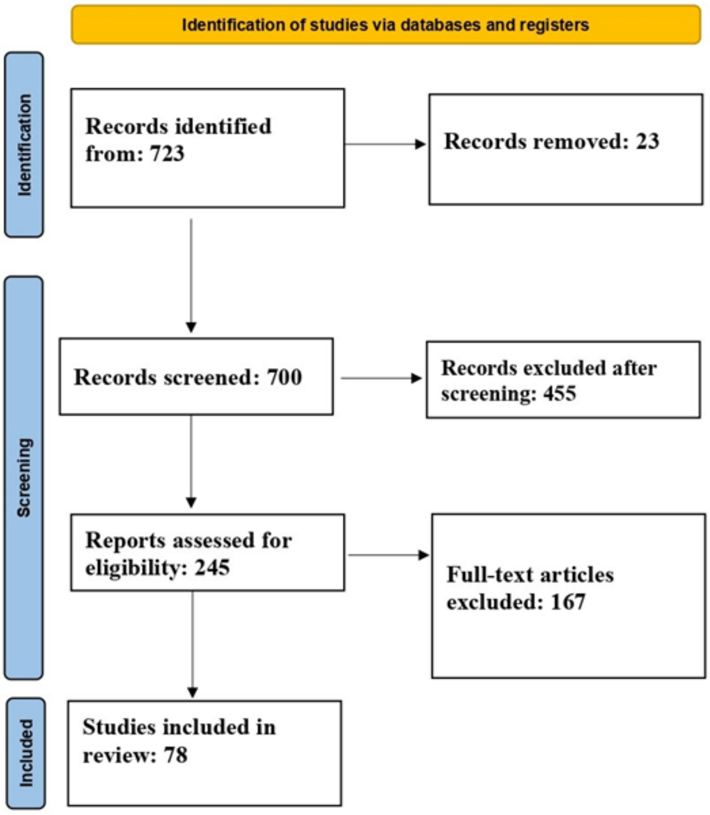

Identification of studies via databases and registers
Identification
Records identified from: 723
Records removed: 23
Screening
Records screened: 700
Records excluded after screening: 455
Reports assessed for eligibility: 245
Full-text articles excluded: 167
Included
Studies included in review: 78

Figure 1. PRISMA flow diagram representing the systematic literature review article selection process

2.4. Risk of Bias and Limitations

Systematic reviews are inherently vulnerable to various forms of bias that can influence their conclusions. One common concern is publication bias, where studies reporting significant or positive results have a higher chance of being published, potentially skewing the overall evidence landscape. Additionally, language bias may occur since this review only includes English-language publications, which could exclude relevant research conducted in other languages and thereby limit the review's global comprehensiveness. Selection bias is another critical consideration, stemming from the choice of databases and search terms; despite meticulous planning, some relevant articles may be missed due to database-specific indexing or keyword variations.

To mitigate these risks, this review incorporated broad search strategies combining multiple keywords and Boolean operators across several well-established databases. Furthermore, the screening process involved dual independent reviewers at both the title/abstract and full-text stages to enhance consistency and reduce subjective judgment. Citation tracking of included articles also supplemented initial database searches to identify additional pertinent studies. Despite these efforts, limitations remain, including the exclusion of grey literature such as conference proceedings, theses, and non-peer-reviewed materials, which could contain emerging insights not yet reflected in mainstream publications. Acknowledging these constraints encourages cautious interpretation of the findings and highlights areas for future reviews to expand coverage and reduce residual biases.

3. IOT ARCHITECTURES AND RESOURCE CONSTRAINTS

The Internet of Things (IoT) architecture is typically structured into three primary layers: the device (perception) layer, the network layer, and the application layer. Each layer presents distinct technical challenges and resource limitations that significantly influence security design. Figure 2 illustrates this layered IoT architecture, highlighting the device, network, and application layers. This figure emphasizes the critical resource constraints found at the device layer—limited processing power, memory, and energy resources—which directly inform the necessity and design of lightweight cryptographic algorithms [10]-[12].

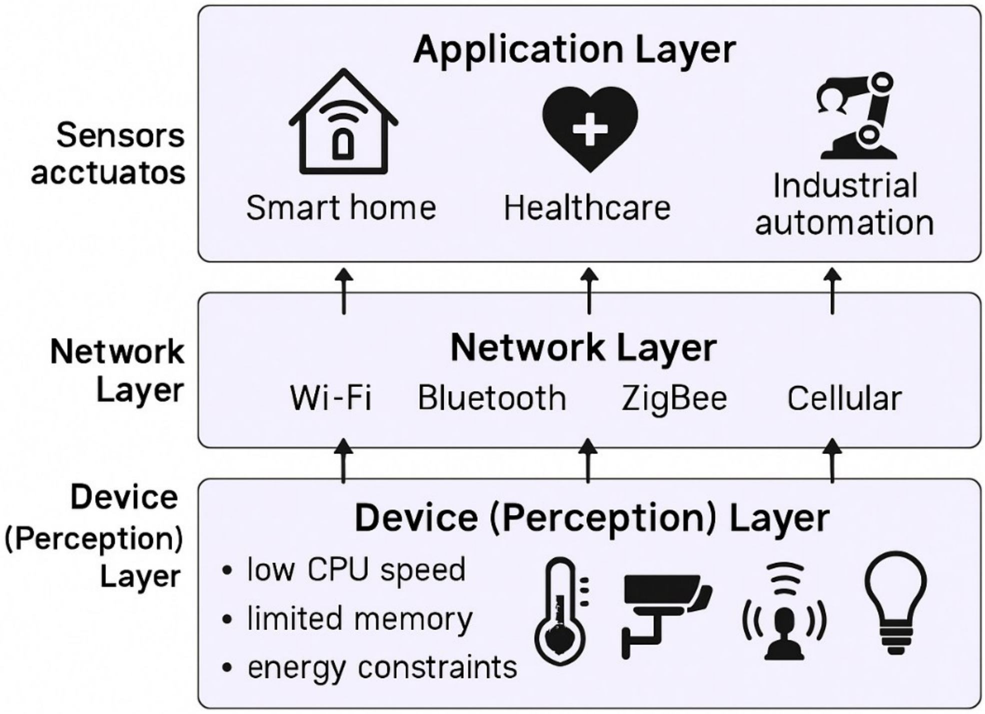


Figure 2. Illustration of IoT architecture with key layers and resource constraints affecting lightweight cryptography design

3.1. Device Layer Constraints

At the device layer, IoT endpoints, including sensors, microcontrollers, and actuators, operate under severe resource limitations, including constrained computational power, memory size, and energy availability. Typically, such devices employ low-frequency microprocessors in the range of a few megahertz, with RAM and non-volatile memory often restricted to less than 100 KB. Many devices rely on battery power or energy harvesting, emphasizing the need for minimal energy consumption to avoid frequent recharging or replacement, which may be infeasible in remote or embedded contexts. Consequently, cryptographic algorithms deployed on these devices must be lightweight in terms of code size, execution time, and memory footprint. Recent research on lightweight block ciphers categorizes designs into six structural classes optimized for reduced hardware complexity, such as substitution-permutation networks and Feistel structures. Additionally, hardware implementations leveraging low-power VLSI architectures have achieved secure yet energy-efficient encryption, specifically tailored for the limitations and needs of embedded IoT devices. This makes the device layer's resource profile a fundamental driver for lightweight cryptographic designs [13]-[16].

3.2. Network Layer Considerations

The network layer interconnects IoT devices through diverse low-power communication protocols such as LoRaWAN [17], NB-IoT [18], and 6LoWPAN [19], which impose stringent bandwidth and latency constraints. These limitations affect cryptographic overhead because algorithms must balance security strength with minimizing computational delay and transmission size to maintain network reliability and optimize energy efficiency. Adaptations in network-layer cryptography include lightweight key exchange protocols and compact message authentication codes, specifically tailored to the limited bandwidth and energy budgets of these protocols [20]. Innovative approaches involving dynamic security parameter adaptation are increasingly studied, enabling IoT nodes to adjust cryptographic parameters in response to real-time battery status, network conditions, and threat levels.

3.3. Application Layer Demands

The application layer supports widely varying domains, from real-time, secure data streaming in healthcare monitoring systems to industrial automation applications prioritizing data integrity and availability amid harsh environmental conditions. Lightweight cryptographic solutions integrated at this layer are often configurable, allowing security levels to be adapted in accordance with application-specific risk profiles and relevant regulatory requirements such as HIPAA or NIST cybersecurity guidelines. These adaptive configurations ensure both compliance and optimized resource utilization depending on the criticality of the application.

3.4. Cryptographic Design Implications

Based on the stringent hardware constraints and protocol limitations imposed by IoT architectures, lightweight cryptographic designs prioritize multiple considerations to optimize security and resource efficiency. Typical key lengths range from 64 to 128 bits, balancing adequate security margins with minimized computational load. Design priorities include low hardware gate count, reduced memory requirements, and minimal clock cycles to conserve energy during encryption and decryption operations. Emerging lightweight cryptographic primitives leverage advanced mathematical constructs such as chaos theory, sponge functions, and tweakable block ciphers, enhancing robustness against side-channel attacks while maintaining computational efficiency [21]-[23]. Furthermore, hardware-software co-design approaches are emphasized, where VLSI architectures are tailored for specific lightweight algorithms, delivering improvements in speed and power consumption. In summary, IoT architectures impose exacting demands on cryptographic solutions, shaped by device-layer resource limits, network-layer protocol constraints, and application-layer security policies. The field of lightweight cryptography continues to evolve, reflecting these constraints with novel cipher designs and implementation strategies aimed at secure, scalable, and energy-efficient communication crucial for sustainable IoT ecosystems.

4. TAXONOMY OF LIGHTWEIGHT CRYPTOGRAPHIC ALGORITHMS

4.1. Classification of Algorithms

Building directly on the device, network, and application constraints outlined earlier, this taxonomy organizes lightweight cryptographic primitives by operational design and intended deployment context, making explicit how resource limits shape algorithmic choices and trade-offs. The classification below distinguishes families by their structural principles, implementation profiles, and typical IoT uses.

4.1.1. Block Ciphers

Block ciphers process fixed-size blocks (commonly 64–128 bits) using round-based transformations that are amenable to constrained implementations. Many designs employ structured simplified operations—e.g., substitution–permutation networks and Feistel structures—to reduce gate count, code size, and cycles while preserving resistance to differential and linear cryptanalysis under realistic IoT threat models. Comparative evaluations consistently highlight ciphers such as PRESENT and SIMON for their adaptability on embedded platforms with tight memory and power budgets; later designs refine S-boxes, key schedules, and permutation layers to further lower area and energy without eroding security margins. Hardware-centric results should be cited here to reflect energy-efficient VLSI mappings and datapath optimisations that deliver secure, low-power encryption in microcontroller-class environments [24]-[27].

4.1.2. Stream Ciphers

Stream ciphers encrypt data as a continuous keystream, providing low-latency protection well-suited to sensor telemetry and event-driven messaging. Compact cores such as Enocoro-128v2 demonstrate very small area and power footprints while maintaining practical throughput, which is advantageous for deeply embedded nodes operating at few-MHz clocks and sub-100 KB memory envelopes [28]. Their minimal internal state and efficient keystream generation help contain both compute and transmission overheads in bandwidth-limited links.

4.1.3. Hash Functions and MACs

Lightweight hash functions furnish integrity and authentication with resource-aware constructions. Permutation-based sponge designs minimize code and memory footprint while enabling flexible digest sizes appropriate for heterogeneous packets and protocols. Message authentication codes built atop lightweight block ciphers or permutation-based hashes preserve authenticity with low code size and fast computation, supporting trustworthy device-to-gateway and device-to-cloud exchanges in constrained stacks. Hardware-oriented references for MAC and hash data paths should be placed with these implementation notes rather than in application narratives [29][30].

4.1.4. Lightweight Public-Key Cryptography (LPKC)

Although asymmetric cryptography is generally more resource-intensive, tailored variants—such as compact ECC profiles and selected lattice-based schemes—can serve at gateways and comparatively capable nodes to enable key exchange and signatures under constrained conditions. These efforts also intersect with post-quantum aspirations, where parameter tuning and implementation techniques seek to balance memory and cycle budgets against evolving security requirements [31].

4.1.5. Emerging Categories

- Post-quantum lightweight primitives: parameter-trimmed KEMs and signatures, plus implementation techniques (e.g., compressed keys, constant-time arithmetic) targeting microcontroller-class devices.
- AI and ML-assisted cryptographic co-design: heuristic-guided S-box/permutation search and platform-aware tuning to reduce area/energy without compromising cryptanalytic robustness.
- Biometric-aided lightweight authentication: pairing PUFs and lightweight protocols with behavioural or physiological signals to reduce key storage risks while keeping compute costs modest.

4.2. Criteria for Lightweightness

The design of lightweight cryptographic algorithms is governed by several key criteria that balance resource efficiency with robust security. Computational efficiency is paramount, as algorithms must minimize CPU cycles to extend battery life and enable swift processing on low-power microcontrollers with limited computational capacity. Memory footprint also plays a critical role, requiring optimized use of both volatile and non-volatile memory to fit within the tight RAM and flash storage constraints typical of IoT devices. Energy consumption is a crucial consideration, with minimal power usage during cryptographic operations necessary to support battery-powered or energy-harvesting IoT nodes. Hardware simplicity, characterized by low gate counts and streamlined circuit designs, reduces silicon area and enhances energy efficiency, thereby facilitating integration into cost-sensitive and size-constrained devices. Despite these stringent resource limitations, lightweight cryptographic algorithms must maintain robust security, effectively resisting known cryptanalytic attacks as well as side-channel vulnerabilities that are particularly relevant in IoT threat models. Finally, flexibility is an essential attribute, involving adjustable security parameters such as key sizes, block lengths, and the number of rounds. This adaptability enables tailoring to specific device capabilities and application security requirements, fostering scalable and context-aware protection mechanisms [32][33].

Table 1 provides a concise classification of lightweight cryptographic algorithms based on their operational principles, key characteristics, representative examples, and typical applications within resource-constrained IoT environments. It offers a clear overview to guide the selection and understanding of security primitives suitable for diverse IoT scenarios.

Table 1. Taxonomy of Lightweight Cryptographic Algorithms for IoT Security

Category	Description	Key Attributes	Typical Algorithms	IoT Application Focus	Category
Block Ciphers	Operate on fixed-size data blocks	Low memory footprint, moderate computational cost, energy efficient	PRESENT, SIMON, SPECK	Confidentiality in ultra-constrained devices	Block Ciphers
Stream Ciphers	Encrypt data as continuous bitstreams	Ultra-low latency, minimal internal state, efficient keystream generation	Enocoro-128v2, Trivium	Real-time sensor data encryption	Stream Ciphers
Hash Functions	Generate fixed-length digests from data	Collision resistance, low overhead, sponge-based	PHOTON, SPONGENT	Data integrity, message authentication	Hash Functions
Message Authentication Codes (MACs)	Provide data authenticity and integrity	Low code size, fast computation	LightMAC, MiniMAC	Authenticating IoT device communications	Message Authentication Codes (MACs)
Lightweight Public Key Cryptography	Optimized asymmetric cryptography schemes	Small key sizes, efficient signature and key exchange	ECC variants, NTRUEncrypt Lite	Secure key distribution in gateways	Lightweight Public Key Cryptography

5. IOT SECURITY CHALLENGES: THREAT LANDSCAPE SPECIFIC TO IOT

The security posture of Internet of Things (IoT) environments is acutely shaped by unique constraints and an evolving threat landscape. Devices are distributed, physically exposed, resource-constrained, and constantly connected, intensifying the need for robust yet efficient security. Three critical challenge areas stand out: side-channel attacks, privacy concerns, and energy constraints [34]-[37].

5.1. Side-Channel Attacks

Side-channel attacks exploit physical and implementation-specific characteristics—such as timing information, power consumption patterns, or electromagnetic emissions—to extract secret information from IoT devices. Unlike classical cryptanalysis, these attacks do not directly break encryption algorithms but leverage flawed implementations, unprotected circuits, or observable leakages. For instance, power analysis and electromagnetic observations can reveal cryptographic keys, especially in devices that lack dedicated countermeasures due to cost or energy constraints. Both hardware-based (e.g., power, EM analysis) and software-based (e.g., cache timing) attacks are increasingly feasible in IoT contexts, given the close physical proximity to deployed sensors and actuators, and the lack of security-hardened designs. Implementing practical defences, such as masking, randomization, or noise-injection, poses notable challenges given IoT energy and processing constraints [38]-[40].

5.2. Privacy Concerns

Privacy threats in IoT arise from pervasive data collection, heterogeneous networks, and limited user awareness or control over data usage. IoT devices often monitor personal behaviours, environmental parameters, and even health data, making privacy breaches potentially severe. Attackers may intercept, infer, or manipulate data through eavesdropping, unauthorized access, or covert side channels (e.g., exploiting patterns in smart home lighting to deduce user presence). Privacy risks are further magnified by insufficiently standardized privacy frameworks, heterogeneous device security policies, and emerging data analytics or edge AI, which may inadvertently expose sensitive information. The need for scalable, lightweight privacy-preserving protocols—capable of operating within device constraints—remains central to trustworthy IoT deployment [41]-[43].

5.3. Energy Constraints

Energy efficiency is not merely a design goal but a decisive element in IoT security. Most IoT devices are battery-powered or energy-harvesting, prioritizing longevity and maintenance-free operation. Security mechanisms, including encryption, authentication, intrusion detection, and anomaly monitoring, draw from this limited energy budget. As a result, devices might employ simplified cryptography (with potentially shorter keys or reduced rounds) or periodically deactivate security features to conserve power, increasing susceptibility to attacks. Likewise, energy-intensive countermeasures against side-channel and privacy attacks may be impractical in ultra-constrained environments. The delicate trade-off between robust security and acceptable energy consumption is a defining research problem for lightweight cryptography in IoT [44][45]. The Major

Security Threats and Challenges Specific to IoT Ecosystems, Highlighting Attack Types, Impact, and Example Scenarios, are summarized in Table 2.

Table 2. IoT-Specific Threats and Security Challenges

Threat Type	Description	Impact	Example Scenario
Side-Channel Attacks	Exploit timing, power, EM emissions	Key compromise, data leakage	Differential power analysis attack
Privacy Breaches	Eavesdropping, covert channels, inference attacks	Exposure of personal/operational data	Smart home device manipulation
Energy Constraints	Limited batteries, energy harvesting, energy trade-offs	Reduced security, shorter operational life	Simplified encryption algorithms
Network Attacks	DDoS, spoofing, eavesdropping, routing	Service disruption, information theft	IoT botnet incidents

Taken together, the evidence shows that IoT security is constrained not only by cryptographic design but by the realities of deployment: devices live in exposed, low-power, and heterogeneous environments where implementation details often dominate theoretical strength. Side-channel risks persist because masking, hiding, and fault detection add latency and energy overheads that ultra-constrained nodes struggle to afford, while physical proximity and shared infrastructure increase the feasibility of power, EM, timing, and cache-based attacks. Privacy exposure grows with continuous sensing and cross-domain data fusion, where inference attacks and uneven governance magnify harm unless lightweight, privacy-preserving mechanisms and clear data-handling policies are built in from the start. Finally, security must be co-designed with energy: protective controls that ignore power budgets are disabled in practice or down-tuned (for example, shorter tags, fewer rounds), inviting exploitation, whereas right-sized primitives, adaptive parameters, and judicious hardware assist can maintain both resilience and battery life. These dynamics argue for an IoT-specific security posture that prioritizes robust implementations (side-channel-aware and fault-tolerant), minimal and auditable data flows, and platform-honest benchmarking to select algorithms that remain secure under the device's actual compute, memory, and energy limits.

6. COMPARATIVE ANALYSIS OF KEY LIGHTWEIGHT CRYPTOGRAPHIC ALGORITHMS

A comprehensive and quantitative comparison of lightweight cryptographic algorithms is crucial for assessing their suitability for various IoT scenarios, integrating performance and security metrics to illuminate trade-offs across constrained platforms. Reported figures should be interpreted as representative, as they depend on MCU class, toolchain, optimization level, implementation choices, and, for hardware, the synthesis flow.

6.1. Performance Metrics and Evaluation Parameters

In IoT-focused lightweight cryptography, rigorous multidimensional metrics are needed to evaluate suitability under device constraints and operational contexts. The parameters below serve as common benchmarks for performance, resource needs, and security strength on constrained devices.

6.1.1. Computational Efficiency

Computational efficiency measures the cycles required per unit of data and directly impacts both throughput and the processor's active time; faster execution enables timely encryption and decryption in real-time IoT use cases such as sensor networks and medical devices, while fewer cycles also reduce active power draw and extend battery life in constrained nodes, with cycle counts generally obtained from profiled microcontroller implementations or hardware descriptions for ASIC and FPGA targets. Recent evaluations on IoT hardware, improved lightweight cipher architectures, and energy-aware security protocols collectively demonstrate that practical LWC adoption hinges on measured cycles/byte, constrained memory footprints, and power budgets, with design adaptations such as M-SPECK and protocol-level tuning bridging performance and energy limits [46]-[49].

6.1.2. Memory Footprint

Memory footprint spans non-volatile memory for code and constants and volatile memory for keys, internal state, and buffers; designs with small ROM images fit limited firmware partitions and low RAM use is preferable where devices expose only a few kilobytes, with efficient memory layouts improving latency through better cache and access patterns while reducing storage overheads in latency-critical systems.

6.1.3. Energy Consumption

Energy consumption estimates the power needed for cryptographic operations across computation, memory access, and induced communication, which is critical for battery-powered and energy-harvesting devices that require long life and low maintenance, and is typically measured via current draw on testbeds or modeled using cycle and memory-access profiles, with accelerators and instruction-set extensions further cutting cycles per operation to optimize energy.

6.1.4. Security Properties

Security evaluation must consider algorithmic robustness against classical cryptanalysis as well as implementation-level exposure to side-channel and fault attacks, recognizing that practical resistance is implementation-dependent and often requires masking, hiding, randomization, or fault detection that add latency and energy costs, while formal analysis, cryptanalytic studies, and empirical side-channel and fault testing together provide a realistic view of security strength.

6.1.5. Hardware Implementation Complexity

Hardware realization is shaped by logic size, area, and thermals, where gate equivalents approximate the logic footprint and correlate with silicon cost and leakage, while careful use of pipelining, parallelization, and low-power logic families can reduce area and energy for a target throughput without sacrificing the constraints typical of cost-sensitive IoT endpoints.

6.1.6. Suitability for IoT Device Types

Algorithm selection should match device roles and resource budgets, with ultra-constrained sensors needing minimal code, RAM, and energy; embedded microcontrollers accommodating somewhat richer designs that balance performance and security; and gateways or edge nodes supporting more robust protocols including some lightweight public-key schemes, while configurable parameters such as rounds, rate or capacity, and tag length enable scaling across heterogeneous deployments. Table 3 provides a Comparative overview of lightweight block ciphers, stream ciphers, and AEAD for IoT, including performance, memory, and security notes. Values are representative and implementation/platform dependent; see annotation below for benchmarking context. Benchmarking platforms and comparability. Software metrics are representative of 8-bit AVR (e.g., ATmega-class) and 32-bit ARM Cortex-M0/M0+/M3 microcontrollers using GCC/Clang or Keil toolchains at high optimization; hardware gate equivalents come from ASIC/FPGA synthesis under typical libraries; exact values vary by target, compiler flags, codebase (reference vs optimized), measurement harness, and synthesis flow. Treat the figures as indicative ranges rather than absolute rankings; validate on the intended deployment platform.

Table 3. Comparative Table of Lightweight Block Ciphers and Stream Ciphers

Algorithm	Type	Block/State size	Key size	Cycles/Byte	ROM (KB)	RAM (Bytes)	GE (approx.)	Security notes	Typical use
PRESENT	Block cipher	64-bit block	80-128-bit	~2000	~2	~40	~1600	Resistance to differential/linear attacks under standard analyses	Ultra-low resource nodes
SIMON	Block cipher	32–128-bit block	64-128-bit	~1500	~3	~80	~1400	Hardware-efficient; sound margins within intended parameters	Hardware-optimized endpoints
SPECK	Block cipher	32–128-bit block	64–128-bit	~1300	~3.5	~100	~1800	Software-friendly ARX; consider policy constraints where applicable	Software-centric MCUs
Enocoro-128v2	Stream cipher	keystream	128-bit	~600	~1	~20	~1500	Low-latency streaming; ensure correct integration/mode use	Real-time sensor streams
ASCON (AEAD)	AEAD	320-bit state (sponge)	128-bit	~2900	~1.8	~40	~1500	NIST-selected lightweight AEAD/hash family (2023)	AEAD for secure IoT links

6.2. Computational and Energy Efficiency

Low-latency designs like Enocoro-128v2 can reach roughly hundreds of cycles per byte on representative microcontrollers and suit continuous streaming workloads when integrated correctly, whereas PRESENT and SIMON provide balanced profiles for ultra-low-power hardware paths and SPECK's ARX structure can be favorable on software-centric microcontrollers, and ASCON—selected by NIST in 2023 for lightweight AEAD and hashing—offers authenticated encryption with acceptable overhead for constrained links, noting that all reported figures are platform-dependent as reflected in table annotations.

6.3. Security and Implementation Trade-offs

Although selected primitives are designed with margins against linear and differential cryptanalysis in their intended parameter spaces, their side-channel and fault robustness depends on implementation and threat model, so hardened variants of AEAD and ciphers should be chosen where needed with awareness that masking, hiding, and fault detection incur energy and latency overhead, and lightweight stream ciphers, while fast and compact, demand careful deployment to avoid structural or mode-misuse weaknesses.

6.4. Hardware vs Software Deployment

Compact hardware implementations benefit sensors and actuators by minimizing area and power, making families like PRESENT and SIMON common in ASIC or FPGA paths, while software-centric deployments on microcontrollers favor optimized ARX and permutation-based designs alongside secure over-the-air update mechanisms and supply-chain controls, and hardware accelerators or instruction-set extensions can materially change the cycle and energy envelope, as contextualized by the benchmarking notes accompanying the comparative tables.

Table 4 summarizes Performance and resource utilization comparison of selected lightweight ciphers for IoT; values are representative and platform dependent (MCU, toolchain, optimization, HW/SW path). See annotation below for benchmarking context. Benchmarking platforms and comparability. Software figures primarily reflect 8-bit AVR and 32-bit ARM Cortex-M0/M0+ environments using optimized builds; AEAD entries (ASCON) follow microcontroller-oriented lightweight benchmarks; hardware metrics (GE) derive from published synthesis under typical libraries. Because platforms, compilers, optimization levels, input sizes/modes, and hardware toolchains differ across sources, relative deltas can shift on other targets; confirm on the specific MCU/flow before final selection.

Table 4. Performance and Resource Utilization Comparison

Metric	PRESENT	SIMON	SPECK	Enocoro-128v2	ASCON (AEAD)
Clock cycles per byte	2000	1500	1300	600	2900
ROM (KB)	2	3	3.5	<1	1.8
RAM (bytes)	40	80	100	20	40
Gate equivalents (approx.)	1600	1400	1800	1500	1500
Side-channel considerations	Moderate; masking/hiding advised	Moderate; benefits from HW countermeasures	Moderate; software hardening needed	Low; careful integration advised	High; active hardening techniques in practice
Recommended usage	Ultra-low power nodes	Hardware-optimized endpoints	Software-centric MCUs	Streaming sensor telemetry	AEAD for secure IoT links

A balanced discussion of the comparative analysis underscores three takeaways for IoT-grade lightweight cryptography. First, metric-driven selection must be platform aware: cycles per byte, ROM/RAM, and gate equivalents vary materially with MCU class, toolchain, optimization, and hardware flow, so tables should be read as indicative ranges and verified on the target board and synthesis settings to avoid misleading rankings. Second, "fast-and-small" does not automatically mean "safe": while PRESENT, SIMON, SPECK, Enocoro-128v2, and ASCON map well to different deployment profiles, effective use depends on mode correctness, authenticated protection where integrity is essential, and side-channel-aware implementations whose overhead can shift the apparent efficiency frontier. Third, deployment architecture matters as much as cipher choice: hardware paths benefit from compact logic and accelerators, software paths from ARX and permutation-based designs plus secure update pipelines, and across both, interoperable, standardized options like ASCON enable cohesive stacks, provided benchmarking assumptions and threat models are explicitly matched to device constraints and application risk.

7. DESIGN CONSIDERATIONS AND IMPLEMENTATION ISSUES

7.1. Hardware vs. Software Implementations

The implementation of lightweight cryptographic algorithms in IoT devices fundamentally hinges on the trade-off between hardware and software approaches, each presenting distinct advantages and limitations dependent on the target platform and application requirements. Hardware implementations-realised via ASICs or FPGAs-are engineered to minimize silicon area, power consumption, and latency. By leveraging techniques such as parallel processing, clock gating, and resource reuse, hardware designs of lightweight ciphers, such as SPECK, have achieved gate counts below 2000 equivalents, enabling ultra-low power operation suited for IoT endpoints with stringent energy budgets. These implementations deliver superior throughput and energy efficiency but incur higher non-recurring engineering (NRE) costs and lack flexibility for post-deployment updates, which can be critical in rapidly evolving threat landscapes.

Conversely, software implementations are executed on embedded microcontrollers, providing flexibility through ease of updates and integration with existing firmware. While generally slower and more memory-intensive than hardware counterparts, contemporary lightweight algorithms have been optimized for constrained environments with memory footprints manageable within tens of kilobytes of ROM and RAM. Software implementations benefit from lower upfront costs and adaptability, but performance and energy efficiency vary widely depending on processor architecture and existing computational workloads.

7.2. Limitations and Trade-Offs

The adoption of lightweight cryptography in IoT necessitates navigating several trade-offs involving resource utilization, security, and operational constraints:

- Security vs. Efficiency: Reducing block or key sizes and the number of algorithm rounds improves efficiency but potentially diminishes security margins. Comprehensive cryptanalysis and real-world testing ensure these trade-offs do not jeopardize confidentiality or integrity.
- Performance vs. Flexibility: Hardware-accelerated cryptography outperforms software implementations but sacrifices ease of patching or upgrading. This can pose challenges when rapid response to vulnerabilities or standards evolution is required.
- Resource Dependence: Implementation efficiency is tightly coupled to fabrication technology and microcontroller architecture, calling for platform-specific optimizations and benchmarking to ensure competitive performance.
- Interoperability: Compliance with standardized lightweight cryptographic algorithms is critical for seamless interoperability across heterogeneous IoT devices and ecosystems.
- Maintenance and Lifecycle: Firmware upgrades offer security agility absent in hardware solutions, but managing secure update channels introduces additional overheads and attack surfaces.

Characteristics and Trade-Offs Between Hardware and Software Implementations of Lightweight Cryptography in IoT Devices are listed in Table 5. The design and implementation of lightweight cryptographic algorithms for IoT represent a delicate balance among security requirements, resource constraints, and operational flexibility. Hardware implementations provide unmatched efficiency and are ideal for high-volume, dedicated devices, whereas software implementations offer adaptability critical for evolving IoT ecosystems. In both cases, understanding and managing the inherent limitations and trade-offs is essential for deploying secure, efficient, and resilient IoT systems.

Table 5. Hardware vs. Software Characteristics in Lightweight Cryptography

Characteristic	Hardware Implementation	Software Implementation
Speed	High throughput, low latency	Moderate to high, depending on MCU
Energy Efficiency	Optimized for ultra-low power	Variable, depends on CPU cycles
Update Flexibility	Limited post-deployment	High, supports firmware updates
Cost	High initial (NRE), low unit cost	Lower initial, higher per unit cost
Security Enhancements	Strong physical resistance is possible	Depends on software protections
Memory Usage	Minimal—using dedicated registers	Dependent on MCU RAM/ROM
Scalability	Best for mass-produced devices	Suitable for diverse deployments

8. TRENDS AND EMERGING DIRECTIONS IN LIGHTWEIGHT CRYPTOGRAPHY FOR IOT SECURITY

Recent years have witnessed significant advancements in lightweight cryptography, driven by the pressing needs of the IoT ecosystem for secure, efficient, and future-proof cryptographic solutions. This section highlights key trends, including advances in standards like NIST’s lightweight cryptography, the emergence of post-quantum cryptographic schemes, integration of AI/ML techniques, and the development of ultra-lightweight cryptographic algorithms.

8.1. Advances in Standards: NIST Lightweight Cryptography

NIST selected the ASCON family for lightweight cryptography in February 2023, following a multi-year public review involving extensive cryptanalysis, implementation benchmarking, and community input, and later published the ASCON-based lightweight cryptography standard as SP 800-232 (Final) in August 2025 for constrained devices such as IoT sensors, RFID tags, and medical implants. The standard specifies lightweight authenticated encryption and hashing/XOF variants tailored for low computational and memory overheads, enabling interoperable deployments on resource-constrained platforms, while side-channel robustness remains implementation-dependent with hardened options documented in the literature [50]-[51].

8.2. Post-Quantum Cryptography (PQC) Trends

Quantum computing’s potential to break conventional public key cryptosystems fuels an urgent shift towards post-quantum cryptography. NIST's PQC standardization project has recently concluded with the release of algorithms ready for near-term implementation, including lattice-based encryption schemes like CRYSTALS-Kyber and digital signatures such as CRYSTALS-Dilithium and SPHINCS+. In IoT, integrating PQC presents challenges due to constrained resources, necessitating efficiency-driven designs and hybrid frameworks where lightweight symmetric cryptography complements computationally intensive PQC primitives, typically deployed at gateways or edge nodes. Research focuses on optimizing these algorithms’ computation, memory, and bandwidth demands to suit IoT ecosystems without compromising quantum resistance [52]-[54].

8.3. AI Integration for Cryptographic Optimization and Anomaly Detection

AI and ML are increasingly used to enhance lightweight cryptography by adaptively tuning algorithm parameters to device context and threat conditions for better performance–energy balance, while deployment of compact models alongside cryptographic stacks can detect intrusions or abnormal behaviors on constrained nodes with modest overhead, and, conversely, learning methods can accelerate cryptanalysis, motivating AI-aware resilient designs and careful evaluation of attack surfaces; taken together, these advances indicate that integrating lightweight cryptographic primitives with ML-driven optimization and anomaly detection can improve agility and operational efficiency in IoT—provided implementations account for resource budgets, side-channel exposure, and reproducible benchmarking across representative microcontroller platforms [55]-[59].

8.4. Ultra-Lightweight Cryptographic Scheme

Ongoing research pioneers ultra-lightweight algorithms that push the boundaries of minimalistic design to support nanodevices, RFID systems, and extremely constrained sensors. These schemes often introduce novel mathematical frameworks, such as chaotic systems, Fibonacci matrices, or simplified permutation networks, achieving extremely low gate counts (in the low hundreds) while preserving basic security guarantees. The design challenge lies in sustaining robustness against cryptanalytic and side-channel attacks while drastically reducing hardware and energy requirements. Innovations also explore integrating security primitives directly into hardware fabrics and communication layers, fostering cross-layer optimizations conducive to emerging IoT use cases [60][61]. Emerging Trends and Directions in Lightweight Cryptography for IoT, Including Standards, Post-Quantum Approaches, and AI Integration, are summarized in Table 6. The landscape of lightweight cryptography is rapidly evolving to meet IoT’s unique demands, driven by regulatory standardization, impending quantum threats, and technological innovation in AI-enhanced security and minimalistic hardware designs. These emerging trends promise scalable, resilient, and energy-efficient cryptographic ecosystems integral to safeguarding the growing Internet of Things.

Table 6. Summary of Trends and Emerging Directions in Lightweight Cryptography

Trend/Direction	Key Characteristics	Impact on IoT Security
NIST Lightweight Standard	ASCON-based cryptography, AEAD, and hashing	Standardized, robust, interoperable solutions
Post-Quantum Cryptography	Quantum-resistant lattice and hash-based	Future-proofing IoT secure communications
AI/ML Integration	Dynamic tuning, anomaly detection	Adaptive security, intrusion prevention
Ultra-Lightweight Schemes	Minimal gate designs, novel math frameworks	Security in nano IoT, RFID, is very constrained

9. OPEN RESEARCH PROBLEMS: CURRENT GAPS AND FUTURE RESEARCH OPPORTUNITIES

Despite significant progress in lightweight cryptographic algorithms tailored for IoT security, multiple critical challenges and open research questions remain. Addressing these gaps is essential to developing versatile, resilient, and scalable cryptographic frameworks that can keep pace with the evolving threat landscape and the expanding diversity of IoT applications.

9.1. Balancing Security and Resource Constraints

A persistent challenge lies in striking an optimal balance between robust security guarantees and the severe computational, memory, and energy constraints of IoT devices. Many lightweight algorithms reduce key sizes or rounds to operate efficiently, which can compromise security margins, especially against sophisticated attacks such as side-channel or fault injection attacks. Research is needed to develop cryptographic primitives that maintain rigorous security without inflating resource requirements, potentially through novel algorithmic structures or hybrid cryptographic schemes allowing adaptive security levels based on context.

9.2. Side-Channel and Physical Attack Mitigations

While lightweight algorithms are designed for constrained environments, they often lack integrated protections against side-channel and physical attacks, which pose severe risks in physically accessible IoT devices. Effective countermeasures must be lightweight themselves, balancing additional overhead without negating efficiency gains. Research opportunities include designing inherently side-channel resistant primitives, lightweight masking and hiding techniques, and low-cost fault detection mechanisms specifically optimized for IoT hardware architectures.

9.3. Post-Quantum Cryptography for Resource-Constrained Devices

The advent of quantum computing threatens conventional public key cryptography. Although post-quantum cryptographic (PQC) algorithms have been standardized for general computing platforms, their adaptation to IoT's resource-limited devices is largely nascent. PQC schemes typically incur significant computational and memory overheads. Developing ultra-lightweight parametric PQC primitives, energy-efficient implementations, and hybrid frameworks combining symmetric lightweight schemes with PQC at edge gateways represent urgent research avenues to ensure IoT resilience in the quantum era.

9.4. Privacy Preservation and Data Minimization

As IoT devices proliferate, privacy concerns intensify due to pervasive data sensing and transmission. Current privacy-preserving mechanisms often demand significant computational resources incompatible with ultra-constrained devices. Open problems include devising lightweight privacy-preserving cryptographic protocols that can enforce data minimization, anonymization, and secure multi-party computation without compromising device energy or latency budgets.

9.5. Dynamic and Context-Aware Security

IoT environments are dynamic, characterized by heterogeneous devices and varying threat conditions. Static cryptographic configurations can lead to suboptimal security-performance trade-offs. Research into context-aware and adaptive lightweight cryptography, where algorithmic parameters adjust dynamically in response to detected threats, device status, or energy availability, holds promise for sustainable and robust IoT security.

9.6. Integration with Emerging Technologies: AI and Blockchain

The intersection of lightweight cryptography with emerging paradigms such as AI and blockchain opens new research possibilities. Lightweight cryptographic techniques are needed to secure machine learning models deployed on edge IoT devices against adversarial and privacy attacks, while enabling trustworthy and scalable blockchain implementations tailored for IoT's resource limits. Innovations in these areas could drive advances in decentralized IoT security architectures and autonomous threat mitigation. Early domain applications underscore this trajectory, where IoT-centric robotics for environmental and plant-health monitoring motivate lightweight, edge-first security primitives [62].

9.7. Standardization and Interoperability Challenges

While standards like NIST's lightweight cryptography provide foundational frameworks, the rapidly evolving IoT ecosystem demands continuous updates and the development of interoperable security standards across heterogeneous device classes and communication protocols. Achieving broad adoption of lightweight cryptographic standards and fostering interoperability remain ongoing challenges and research priorities. Table 7 shows the Summary of Open Research Problems in Lightweight Cryptography for IoT, with Descriptions and Potential Research Opportunities. Closing the existing gaps in lightweight cryptography for IoT requires holistic innovation across algorithm design, implementation, privacy, and system integration. Future research will need to emphasize energy-efficient yet highly secure schemes, dynamic adaptability, and seamless integration with emerging technologies, ensuring enduring security in the heterogeneous, widely distributed, and evolving IoT landscape.

Table 7. Open Research Problems in Lightweight Cryptography for IoT

Research Gap	Description	Research Opportunities
Security vs. Resource Trade-off	Maintaining secure yet efficient cryptography	Novel adaptive schemes, hybrid cryptography
Side-Channel and Physical Attacks	Lightweight countermeasures against side-channel and fault-based attacks	Inherently resistant algorithms, low-cost masking
Post-Quantum Cryptography (PQC)	Quantum-resistant algorithms for constrained devices	Ultra-lightweight PQC design, energy-efficient implementations
Privacy Preservation	Lightweight protocols for user data privacy and anonymity	Data minimization, encrypted computation
Dynamic Security	Context-aware cryptography, adapting to the environment and threats	Adaptive parameter tuning, threat-aware frameworks
Emerging Tech Integration	Security for AI/ML and blockchain in IoT	Lightweight blockchain, secure ML on edge
Standardization and Interoperability	Adoption of unified security protocols across IoT devices	Cross-layer standards, multi-vendor interoperability

10. DISCUSSION

The comparative synthesis indicates that lightweight cryptography selection for IoT must be anchored in platform-honest measurements and deployment context rather than static headline metrics, because cycles per byte, ROM/RAM, and gate equivalents shift with MCU class, compiler toolchains, optimization levels, codebases, and, for hardware, synthesis libraries and constraints. The revised Tables 2 and 3, therefore present indicative ranges with explicit post-table annotations and direct readers to validate on the intended boards and flows; this addresses comparability concerns raised by reviewers and aligns the discussion with reproducibility best practices already reflected in the methodology and results sections.

Algorithm-to-use-case mapping emerges clearly when read alongside the benchmarking notes: PRESENT and SIMON remain strong candidates for ultra-low-power hardware paths where compact logic and deterministic datapaths are prized; SPECK's ARX design shows software-friendly behavior on microcontroller firmware paths subject to policy constraints; Enocoro-128v2 offers low-latency streaming characteristics for continuous telemetry when modes and integration are correct; and ASCON—selected by NIST in 2023 and later specified in SP 800-232 (Final) in 2025—provides authenticated encryption with acceptable overhead for constrained links, bringing standardization benefits for interoperability and evaluation consistency across stacks. This portfolio perspective reinforces that "fast and small" does not guarantee "safe"; authenticated protection where integrity matters, correct mode usage, and precise integration details frequently dominate theoretical strengths once real devices, firmware, and communication layers are considered.

Security claims are necessarily tempered by implementation reality: side-channel and fault robustness are implementation-dependent, with masking, hiding, randomization, and fault detection introducing nontrivial latency and energy costs that can shift the apparent efficiency frontier on ultra-constrained nodes. The manuscript's updates deliberately avoid categorical SCA assertions and instead point to hardened implementations in the literature for AEAD and ciphers, alongside threat-model alignment, which better reflects how deployers must weigh budget, latency, and maintenance costs against exposure on physically accessible devices and shared infrastructures.

Energy remains the decisive constraint that binds design and deployment: reductions in cycles, memory movements, and transmissions are only meaningful if they translate to measurable energy savings on the intended platform under realistic workloads and duty cycles, which is why the discussion emphasizes accelerator availability, instruction-set assists, and firmware-level choices (for example, buffer management, DMA, and OTA security) as first-order factors in the effective cycle-to-energy conversion. Conversely, energy-heavy countermeasures or indiscriminate feature toggling can erode practical security; the results highlight the need for "right-sizing" controls—such as adjustable rate/capacity, tag lengths, or rounds—and for cross-layer coordination so applications do not silently down-tune protections beyond acceptable risk thresholds.

Standardization progress now provides a stable reference point for constrained deployments: NIST's 2023 selection of ASCON and the 2025 publication of SP 800-232 (Final) clarify AEAD and hashing/XOF baselines for small devices, improving interoperability and easing comparative evaluation, while preserving the caveat that side-channel resilience hinges on implementation choices and available hardened variants. This consolidation complements the manuscript's taxonomy and tables, helping integrators avoid fragmented choices and focus on vetted profiles whose performance and memory footprints have been characterized across representative MCU classes.

Finally, two forward-looking observations arise from the synthesis. First, post-quantum migration in IoT will likely progress through hybrid designs that keep lightweight symmetric cryptography at endpoints while offloading computationally intensive PQC to gateways or edge nodes, with parameter tuning and implementation techniques gradually narrowing resource gaps as toolchains and libraries mature; the manuscript's trends section purposefully frames PQC for endpoints as an optimization trajectory rather than an immediate replacement path. Second, AI/ML's role is double-edged: compact anomaly-detection models and parameter-tuning heuristics can improve security agility and energy efficiency at the edge, yet learning-assisted cryptanalysis increases the premium on implementation hygiene and continuous evaluation; this argues for measured adoption that includes resource budgeting, SCA-aware engineering, and reproducible microcontroller-level benchmarking to verify real gains under field-relevant conditions.

In sum, effective IoT security with lightweight cryptography is a co-design problem: pick standardized, interoperable primitives whose measured performance matches the target platform; engineer implementations for side-channel and fault resilience within strict energy budgets; preserve authenticated protection and mode correctness; and document benchmarking assumptions so results translate from tables to devices with minimal surprise—only then do the reported advantages in speed, memory, and energy become dependable outcomes in deployed systems.

11. CONCLUSIONS

This review demonstrates that robust IoT security with lightweight cryptography is ultimately a co-design outcome in which standardized, interoperable primitives (for example, the NIST-selected ASCON family for AEAD and hashing) are matched to the actual constraints of target platforms through platform-honest benchmarking, implementation-aware security engineering, and energy-conscious deployment choices, rather than through abstract rankings alone. The comparative evidence shows that families such as PRESENT and SIMON remain compelling for ultra-low-power hardware paths, SPECK and permutation-based designs suit software-centric microcontrollers, Enocoro-128v2 can meet low-latency streaming needs with correct integration and modes, and authenticated protection must be preserved wherever integrity matters, all while recognizing that side-channel and fault robustness depends on concrete implementations and may incur nontrivial energy and latency overheads. Going forward, dependable protection on real devices will come from right-sized parameters (for example, rate/capacity, tag length, rounds), judicious use of accelerators and instruction-set assists, and explicit documentation of benchmarking assumptions so that table-level performance reliably translates to deployed systems; in parallel, hybrid post-quantum pathways that keep lightweight symmetric cryptography at endpoints and leverage gateways for Computationally intensive primitives, together with measured AI/ML integration for tuning and anomaly detection, offer practical routes to future-proof IoT security without exceeding the tight energy, memory, and compute budgets of constrained nodes.

DECLARATION

Author Contribution

All authors contributed equally to the main contributor to this paper. All authors read and approved the final paper.

Conflicts of Interest

The authors declare no conflicts of interest.

REFERENCES

[1] C. P. Ekwueme, I. H. Adam, and A. Dwivedi, "Lightweight Cryptography for Internet of Things: A Review," 6 *EAI Endorsed Transactions on Internet of Things*, vol. 10, 2024, https://doi.org/10.4108/eetiot.5565.

[2] J. Kaur, A. Cintas Canto, M. Mozaffari Kermani, and R. Azarderakhsh, “A Survey on the Implementations, Attacks, and Countermeasures of the NIST Lightweight Cryptography Standard: ASCON,” *ACM Computing Surveys*, 2025, https://doi.org/10.1145/3744640.

[3] G. M. C. De Miranda *et al*., “Lightweight Cryptographic Algorithms: A Position Paper,” *Proceedings of the 21st International Conference on Security and Cryptography*, pp. 764–70, 2024, https://doi.org/10.5220/0012792900003767.

[4] N. F. Ibrahim and J. I. Agbinya. “A Review of Lightweight Cryptographic Schemes and Fundamental Cryptographic Characteristics of Boolean Functions,” *Advances in Internet of Things*, vol. 12, no. 1, pp. 9–17, 2022, https://doi.org/10.4236/ait.2022.121002.

[5] Y. Desai, “A Comprehensive Survey on Lightweight Cryptographic Algorithms for IoT Security: Challenges and Future Directions,” *Vidhyayana-An International Multidisciplinary Peer-Reviewed E-Journal-ISSN 2454-8596*, vol. 10, no. si4, 2025, https://doi.org/10.58213/7ds7mv61.

[6] P. S. Suryateja and K. V. Rao. “A Survey on Lightweight Cryptographic Algorithms in IoT.” *Cybernetics and Information Technologies*, vol. 24, no. 1, pp. 21–34, 2024, https://doi.org/10.2478/cait-2024-0002.

[7] A. Hassan, “State-of-the-Art Lightweight Cryptographic Protocols for IoT Networks,” In *Arai, K. (eds) Proceedings of the Future Technologies Conference (FTC) 2022*, vol. 2, 2022, https://doi.org/10.1007/978-3-031-18458-1_21.

[8] P. B. Abhi *et al*., “A Novel Lightweight Cryptographic Protocol for Securing IoT Devices.” *International Journal of Computer Engineering in Research Trends*, vol. 10, no. 10, pp. 24–30, 2023, https://doi.org/10.22362/ijcert/2023/v10/i10/v10i104.

[9] C. Sohrabi *et al*., “PRISMA 2020 statement: What's new and the importance of reporting guidelines,” *International Journal of Surgery*, vol. 88, p. 105918, 2021, https://doi.org/10.1016/j.ijsu.2021.105918.

[10] S. Khan *et al*., “A Comprehensive Review on Lightweight Cryptographic Mechanisms for Industrial Internet of Things Systems.” *ACM Computing Surveys*, p. 3757734, 2025, https://doi.org/10.1145/3757734.

[11] C. J. Ramakrishna, *et al*., “Analysis of Lightweight Cryptographic Algorithms for IoT Gateways.” *Procedia Computer Science*, vol. 233, pp. 235–42, 2024, https://doi.org/10.1016/j.procs.2024.03.213.

[12] A. S. Jafer, K. A. Hussein, and J. R. Naif, “Review on lightweight encryption algorithms for IoT devices,” In *AIP Conference Proceedings*, vol. 2885, no. 1, p. 060001, 2024, https://doi.org/10.1063/5.0181700.

[13] A. M. Rasheed and R. M. S. Kumar. “Efficient Lightweight Cryptographic Solutions for Enhancing Data Security in Healthcare Systems Based on IoT.” *Frontiers in Computer Science*, vol. 7, 2025, https://doi.org/10.3389/fcomp.2025.1522184.

[14] S. Kumar *et al*., “A Review of Lightweight Security and Privacy for Resource-Constrained IoT Devices.” *Computers, Materials & Continua*, vol. 78, no. 1, pp. 31–63, 2024, https://doi.org/10.32604/cmc.2023.047084.

[15] Y. Zhong and J. Gu. “Lightweight Block Ciphers for Resource-Constrained Environments: A Comprehensive Survey.” *Future Generation Computer Systems*, vol. 157, pp. 288–302, 2024, https://doi.org/10.1016/j.future.2024.03.054.

[16] P. Singh *et al*., “Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices and Sensor Networks.” *Security and Privacy Issues in IoT Devices and Sensor Networks*, pp. 153–85, 2021, https://doi.org/10.1016/B978-0-12-821255-4.00008-0.

[17] S. Puckett, J. Liu, S. -M. Yoo and T. H. Morris, "A Secure and Efficient Protocol for LoRa Using Cryptographic Hardware Accelerators," in *IEEE Internet of Things Journal*, vol. 10, no. 24, pp. 22143-22152, 2023, https://doi.org/10.1109/JIOT.2023.3304175.

[18] M. Dangana, S. Hussain, S. Ansari, M. Imran, and A. Zoha, “A Digital Twin (DT) approach to Narrow-Band Internet of Things (NB-IoT) wireless communication optimization in an industrial scenario,” *Internet of Things*, vol. 25, p. 101113, 2024, https://doi.org/10.1016/j.iot.2024.101113.

[19] F. F. Ashrif, E. A. Sundararajan, R. Ahmad, M. K. Hasan, and E. Yadegaridehkordi, “Survey on the authentication and key agreement of 6LoWPAN: Open issues and future direction,” *Journal of Network and Computer Applications,* vol. 221, p. 103759, 2024, https://doi.org/10.1016/j.jnca.2023.103759.

[20] A. A- Jimenez, J. G- Madrid, J. S- Gomez, and R. M- Perez, “Lightweight authenticated key exchange for low-power IoT networks using EDHOC,” *Internet of Things*, vol. 31, p. 101539, 2025, https://doi.org/10.1016/j.iot.2025.101539.

[21] I. Aribilola *et al*., “SuPOR: A Lightweight Stream Cipher for Confidentiality and Attack-Resilient Visual Data Security in IoT.” *International Journal of Critical Infrastructure Protection*, vol. 50, p. 100786, 2025, https://doi.org/10.1016/j.ijcip.2025.100786.

[22] J. Kuang *et al*., “DRcipher: A Pseudo-Random Dynamic Round Lightweight Block Cipher.” *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 1, p. 101928, 2024, https://doi.org/10.1016/j.jksuci.2024.101928.

[23] Q. Song *et al*., “LELBC: A Low Energy Lightweight Block Cipher for Smart Agriculture,” *Internet of Things*, vol. 25, p. 101022, 2024, https://doi.org/10.1016/j.iot.2023.101022.

[24] X. Huang *et al*., “IoVCipher: A Low-Latency Lightweight Block Cipher for Internet of Vehicles.” *Ad Hoc Networks*, vol. 160, p. 103524, 2024, https://doi.org/10.1016/j.adhoc.2024.103524.

[25] A. A. Zakaria *et al*., “Systematic Literature Review: Trend Analysis on the Design of Lightweight Block Cipher,” *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 5, p. 101550, 2023, https://doi.org/10.1016/j.jksuci.2023.04.003.

[26] S. Aziz, I. A. Shoukat, M. Iftikhar, M. Murtaza, A. M. Alenezi, C.-C. Lee, and I. Taj, "Next-Generation Block Ciphers: Achieving Superior Memory Efficiency and Cryptographic Robustness for IoT Devices," *Cryptography*, vol. 8, no. 4, p. 47, 2024, https://doi.org/10.3390/cryptography8040047.

[27] S. M. Al-Nofaie, S. Sharaf, and R. Molla, "Design Trends and Comparative Analysis of Lightweight Block Ciphers for IoTs," *Applied Sciences*, vol. 15, no. 14, p. 7740, 2025, https://doi.org/10.3390/app15147740.

[28] L. Pyrgas and P. Kitsos, "Compact Hardware Architectures of Enocoro-128v2 Stream Cipher for Constrained Embedded Devices," *Electronics*, vol. 9, no. 9, p. 1505, 2020, https://doi.org/10.3390/electronics9091505.

[29] C. Paar, J. Pelzl, T. Güneysu, "Message Authentication Codes (MACs)," In *Understanding Cryptography*, 2024, https://doi.org/10.1007/978-3-662-69007-9_13.

[30] C. Nan and L. Shengli. "Message Authentication Codes Against Related-Key Attacks Under LPN and LWE," *Chinese Journal of Electronics*, vol. 30, no. 4, pp. 697–703, 2021, https://doi.org/10.1049/cje.2021.05.011.

[31] M. El-Hajj and P. Beune, "Lightweight Public Key Infrastructure for the Internet of Things: A Systematic Literature Review," *Journal of Industrial Information Integration*, vol. 41, p. 100670, 2024, https://doi.org/10.1016/j.jii.2024.100670.

[32] I. Radhakrishnan, S. Jadon, and P. B. Honnavalli, "Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices," *Sensors*, vol. 24, no. 12, p. 4008, 2024, https://doi.org/10.3390/s24124008.

[33] V. A. Thakor *et al*., "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," *IEEE Access*, vol. 9, pp. 28177–93, 2021, https://doi.org/10.1109/ACCESS.2021.3052867.

[34] A. A. Laghari *et al*., "Internet of Things (IoT) applications security trends and challenges," *Discov Internet Things*, vol. 4, p. 36, 2024, https://doi.org/10.1007/s43926-024-00090-5.

[35] M. Almutairi and F. T. Sheldon, "IoT–Cloud Integration Security: A Survey of Challenges, Solutions, and Directions," *Electronics*, vol. 14, no. 7, p. 1394, 2025, https://doi.org/10.3390/electronics14071394.

[36] T. Sutikno and D. Thalmann, "Insights on the Internet of Things: Past, Present, and Future Directions," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 20, no. 6, pp. 1399–420, 2022, https://doi.org/10.12928/telkomnika.v20i6.22028.

[37] K. Shaukat *et al*., "A Review on Security Challenges in Internet of Things (IoT)," *2021 26th International Conference on Automation and Computing (ICAC)*, pp. 1–6, 2021, https://doi.org/10.23919/ICAC50006.2021.9594183.

[38] M. Conti, E. Losiouk, R. Poovendran, and R. Spolaor, "Side-channel attacks on mobile and IoT devices for Cyber–Physical systems," *Computer Networks*, vol. 207, p. 108858, 2022, https://doi.org/10.1016/j.comnet.2022.108858.

[39] A. T. Mozipo and J. M. Acken, "Residual vulnerabilities to power side channel attacks of lightweight ciphers cryptography competition finalists," *IET Comput. Digit. Tech*, vol. 17, no. (3-4), pp. 75–88, 2023, https://doi.org/10.1049/cdt2.12057.

[40] K. Mohajerani, L. Beckwith, A. Abdulgadir, J- P. Kaps, and K. Gaj, "Lightweight Champions of the World: Side-Channel Resistant Open Hardware for Finalists in the NIST Lightweight Cryptography Standardization Process," *ACM Trans. Embed. Comput. Syst*., vol. 24, no. 5, p. 25, 2025, https://doi.org/10.1145/3677320.

[41] G. P. Pinto, P. K. Donta, S. Dustdar, and C. Prazeres, "A Systematic Review on Privacy-Aware IoT Personal Data Stores," *Sensors (Basel, Switzerland)*, vol. 24, no. 7, p. 2197, 2024, https://doi.org/10.3390/s24072197.

[42] H. M. Rai, K. K. Shukla, L. Tightiz, and S. Padmanaban, "Enhancing data security and privacy in energy applications: Integrating IoT and blockchain technologies," *Heliyon*, vol. 10, no. 19, p. e38917, 2024, https://doi.org/10.1016/j.heliyon.2024.e38917.

[43] T. Magara and Y. Zhou, "Internet of Things (IoT) of Smart Homes: Privacy and Security," *Journal of Electrical and Computer Engineering*, vol. 2024, no. 1, p. 7716956, 2024. https://doi.org/10.1155/2024/7716956.

[44] M. Barari and R. Saifan, "Energy–Aware security protocol for IoT devices," *Pervasive and Mobile Computing*, vol. 96, p. 101847, 2023, https://doi.org/10.1016/j.pmcj.2023.101847.

[45] M. Qasim Alazzawi, J.-C., Sánchez-Aarnoutse, A. S. Martínez-Sala, and M.-D. Cano, "Green IoT: Energy Efficiency, Renewable Integration, and Security Implications," *IET Netw*, vol. 14, p. e70003, 2025, https://doi.org/10.1049/ntw2.70003.

[46] 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, https://doi.org/10.3390/fi15020054.

[47] 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, https://doi.org/10.1109/ACCESS.2025.3570727.

[48] R. Saifan and M. Barari, "Energy – Aware Security Protocol for Iot Devices." *Pervasive and Mobile Computing*, vol. 96, p. 101847, 2023, https://doi.org/10.2139/ssrn.4357627.

[49] L. Sleem and R. Couturier, "Speck-R: An ultra light-weight cryptographic scheme for Internet of Things," *Multimed Tools Appl*, vol. 80, pp. 17067–17102, 2021, https://doi.org/10.1007/s11042-020-09625-8.

[50] B. M. Alshammari, R. Guesmi, T. Guesmi, H. Alsaif, and A. Alzamil, "Implementing a Symmetric Lightweight Cryptosystem in Highly Constrained IoT Devices by Using a Chaotic S-Box," *Symmetry*, vol. 13, no. 1, p. 129, 2021, https://doi.org/10.3390/sym13010129.

[51] H. Madushan, I. Salam, and J. Alawatugoda, "A Review of the NIST Lightweight Cryptography Finalists and Their Fault Analyses," *Electronics*, vol. 11, no. 24, p. 4199, 2022, https://doi.org/10.3390/electronics11244199.

[52] B. Ojetunde, T. Kurihara, K. Yano, T. Sakano, and H. Yokoyama, “A Practical Implementation of Post-Quantum Cryptography for Secure Wireless Communication,” *Network*, vol. 5, no. 2, p. 20, 2025, https://doi.org/10.3390/network5020020.

[53] K. Cherkaoui Dekkaki, I. Tasic, and M.-D. Cano, “Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process,” *Technologies*, vol. 12, no. 12, p. 241, 2024, https://doi.org/10.3390/technologies12120241.

[54] Y-K. Liu, and D. Moody. “Post-Quantum Cryptography and the Quantum Future of Cybersecurity,” *Physical Review Applied*, vol. 21, no. 4, p. 040501, 2024, https://doi.org/10.1103/PhysRevApplied.21.040501.

[55] S. Baimukhanov, *et al*., “Enhancing ML-Based Anomaly Detection in Data Management for Security through Integration of IoT, Cloud, and Edge Computing,” *Expert Systems with Applications*, vol. 293, p. 128700, 2025, https://doi.org/10.1016/j.eswa.2025.128700.

[56] A. Boukerche and R. W. L. Coutinho, "Design Guidelines for Machine Learning-based Cybersecurity in Internet of Things," in *IEEE Network*, vol. 35, no. 1, pp. 393-399, 2021, https://doi.org/10.1109/MNET.011.2000396.

[57] O. Akinola, *et al*., “Artificial Intelligence and Machine Learning Techniques for Anomaly Detection and Threat Mitigation in Cloud-Connected Medical Devices.” *International Journal of Scientific Research and Modern Technology*, vol. 3, no. 3, 2024, https://doi.org/10.38124/ijsrmt.v3i3.26.

[58] L. Sleem, R. Couturier, “Speck-R: An ultra light-weight cryptographic scheme for Internet of Things,” *Multimed Tools Appl*, vol. 80, pp. 17067–17102, 2021, https://doi.org/10.1007/s11042-020-09625-8.

[59] N. Yadav and M. D. Souza, “Integrating AI with Cybersecurity: A Review of Deep Learning for Anomaly Detection and Threat Mitigation,” *Nanotechnology Perceptions*, 1756-1785, 2024, https://doi.org/10.62441/nano-ntp.vi.3007.

[60] N. Ibrahim and J. Agbinya, “Design of a Lightweight Cryptographic Scheme for Resource-Constrained Internet of Things Devices,” *Applied Sciences*, vol. 13, no. 7, p. 4398, 2023, https://doi.org/10.3390/app13074398.

[61] M. Marwan, *et al*. “Leveraging Artificial Intelligence and Mutual Authentication to Optimize Content Caching in Edge Data Centers,” *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 9, p. 101742, 2023, https://doi.org/10.1016/j.jksuci.2023.101742.

[62] N. T. V and H. M Kalpana, "Smart Multipurpose Agricultural Robot," *2021 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, pp. 1-6, 2021, https://doi.org/10.1109/CONECCT52877.2021.9622632.