Iraqi Journal of Information and Communications Technology(**IJICT**)
Vol. 8, Issue 3, December 2025

www.ijict.edu.iq

ISSN:2222-758X
e-ISSN:2789-7362

COMPREHENSIVE REVIEW OF NIST LIGHTWEIGHT CRYPTOGRAPHY ALGORITHMS FOR IOT: PERFORMANCE EVALUATION, ATTACKS, OPTIMIZATIONS, AND PROTOCOL INTEGRATION

Hussein A. Al-shmailawi[1], **Emad H. Al-Hemiary**[2], **Axel Sikora**[3]

[1] Department of Information and Communication Engineering, College of Information Engineering,
Al-Nahrain University, Jadriya, Baghdad, Iraq

[2] Department of Computer Networks Engineering, College of Information Engineering, Al-Nahrain University,
Jadriya, Baghdad, Iraq

[3] Institute of Reliable Embedded Systems and Communication Electronics, Offenburg University, Offenburg,
Germany

hussein.ali@coie-nahrain.edu.iq[1], emad@coie-nahrain.edu.iq[2], axel.sikora@hs-offenburg.de[3]

Corresponding Author: **Axel Sikora**

Received:04/06/2025; Revised:17/07/2025; Accepted:03/12/2025

DOI:**10.31987/ijict.8.3.336**

***Abstract*- The Internet of Things (IoT) is rapidly expanding into critical healthcare, industrial, and commercial domains, yet its resource-constrained devices remain vulnerable to cyberattacks. IoT devices have resource constraints, making it challenging to execute standard security algorithms. To address these limitations, the National Institute of Standards and Technology (NIST) selected 10 Lightweight Cryptographic (LWC) finalist algorithms in 2023 to provide suitable confidentiality for constrained environments. This review focuses exclusively on these finalists and highlights their importance in modern IoT security. A systematic search was conducted across IEEE Xplore, ScienceDirect, Springer, and the Cryptology ePrint Archive, using the PRISMA methodology, defined keywords, and strict inclusion/exclusion criteria. In the initial 2118 retrieved studies, 40 high-quality contributions were selected after title, abstract, and full-text screening. The selected works were categorized into four themes: performance evaluation across hardware and software platforms, cryptanalytic and security assessments, algorithmic optimization, and integration of LWC algorithms into existing systems and communication protocols. Performance analysis research indicates that TinyJambu is the most energy-efficient among the NIST block-cipher-based algorithms. Xoodyak and ASCON demonstrated the best energy efficiency among permutation-based algorithms. On the other hand, the set of Elephant, ISAP, and Grain128-AEAD was the least energy-efficient, consuming up to 10 to 25 times more energy than the most efficient set, TinyJambu. In particular, the first reported cryptanalytic break of the 7-round Xoodyak, presented in a recent article, substantially expands the threat model for the NIST LWC finalist. Some experimental reports indicate a full key-recovery attack with success rates exceeding 90%. In contrast, adapted variants of the attack have proven effective against multiple Elephant-family ciphers, illustrating the importance of updated security assessments and implementation countermeasures. Finally, this study identifies critical research gaps that require further investigation, emphasizing the importance of addressing these challenges through targeted research efforts and developing adaptive solutions in future studies.**

***keywords:* Lightweight cryptography, NIST, IoT, Comprehensive review, Cryptanalysis attacks.**

I. INTRODUCTION

The Internet of Things (IoT) is an infrastructure whereby tangible devices connect to the internet and communicate with each other using embedded devices like sensors and actuators [1]. IoT devices enable automation, remote processes, data collection, and analytics, and produce workflows to optimize operations and more. It is revolutionizing several industries, including healthcare, agriculture, transportation, and the industrial sector, and these characteristics have enormous potential to enhance sustainable social and economic development [2]. For instance, an IoT-enabled intelligent transportation network will raise public safety and security, lower expenses, and increase productivity [3]. IoT is revolutionizing many facets of healthcare, including the ability to deliver online patient care, a benefit to patients, their families, medical professionals, and insurance companies [4]. Similarly, the industrial sector uses IoT to update infrastructure, improve operational reliability and efficiency, give customers access to affordable energy, and enable the industry to track and monitor energy sources [5]. IoT presents serious security risks even though it offers many opportunities for digital transformation. These risks include botnets, distributed denial-of-service attacks, privacy and confidentiality violations, and malware specifically designed for the IoT. To guarantee confidentiality and integrity, IoT data must be authenticated and encrypted as it travels across the network. As a result, encryption tools for protecting private and essential data are insufficient [6].

It is essential to secure IoT data, which is attracting significant attention from the research and industry communities due to the rise in IoT-born attacks. Generally speaking, cryptographic techniques that ensure the confidentiality of encrypted data and the integrity of plaintext information are the primary foundation for security. The energy, power consumption, and throughput of IoT devices are limitations. As a result, the computational cost of traditional cryptographic techniques may be prohibitive for communicating limited hardware needs. The National Institute of Standards and Technology (NIST) emphasized the significance of Lightweight Cryptography (LWC), particularly for enhancing IoT device security. This study, containing a review of promising cryptography algorithms as IoT security solutions, has resulted from these challenges. LWC is appropriate for IoT applications with resource, power, and energy constraints and promises greater efficiency and security than traditional cryptography. In other words, it provides confidentiality and authenticity services with minimal resources [7].

The focus on NIST's finalists is justified by their strict selection process, which includes extensive evaluations of both security and performance. NIST's role in standardizing cryptographic algorithms ensures that the finalists have been carefully evaluated, making them suitable candidates for applications use. The LWC project standard is an innovative approach for selecting standard algorithms since the adoption of the Advanced Encryption Standard (AES). This project further highlights its importance and is expected to have a significant impact in the coming years, opening up many new areas for research. This review explores the latest LWC advancements for the IoT. This review covers the field of LWC applications and focuses on cryptanalytic attacks, contributions to optimization and improvement, and findings from their integration into LWC-based security protocols and systems. Grounded in a comprehensive literature review, this study provides a critical security analysis and thoroughly examines existing LWC benchmarks. Furthermore, it elucidates the key benefits of incorporating LWC into IoT security protocols while addressing associated challenges.

A. Research Gaps

The literature lacks a systematic review that comprehensively compares the lightweight cryptographic algorithms that have reached the NIST finallist in terms of performance across constrained platforms (software on microcontrollers and hardware implementations) on Field-Programmable Gate Array (FPGA), as well as security robustness against a wide range of attacks (differential/linear analysis and side-channel attacks). This review aims to gather performance metrics, attacks, and optimizations; identify which algorithms failed to withstand attacks; document attempts to improve algorithm performance; and provide evidence-based recommendations for selecting the algorithm based on application constraints.

B. Scope of review

This review concentrates on the most significant research papers in LWC. The research will focus exclusively on LWC algorithms that have advanced to the finalists of the NIST competition. This study will investigate the main contributions of these 10 algorithms. Fig. 1 illustrates the scope of review.

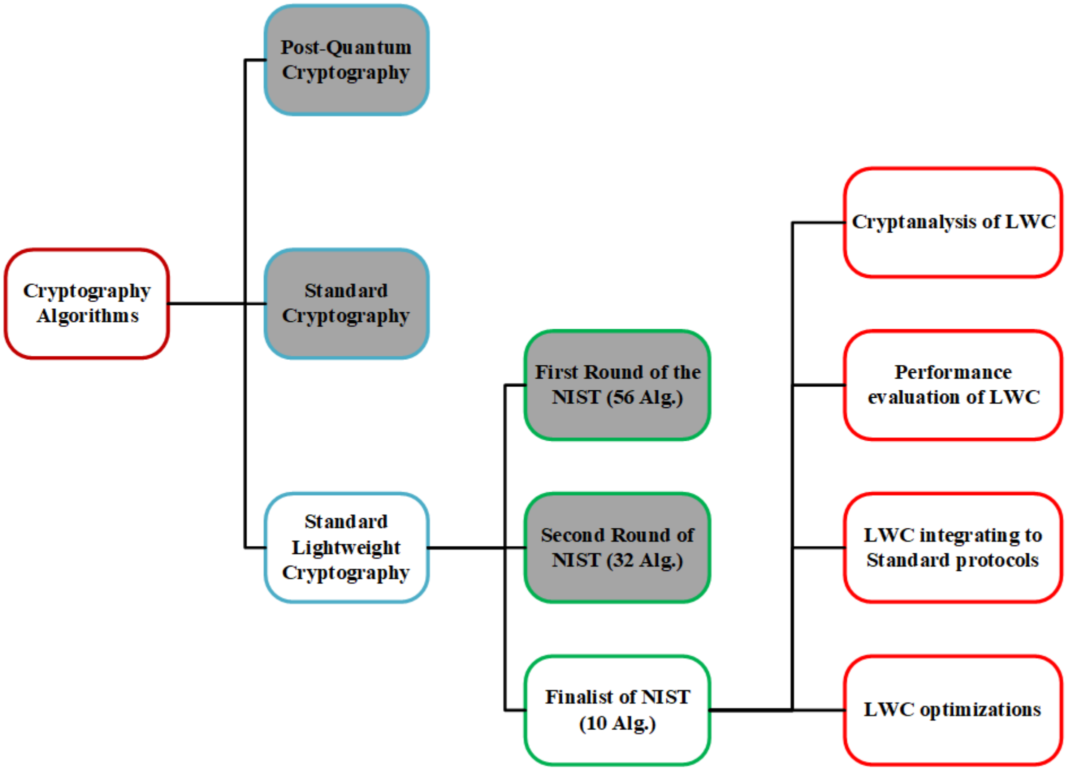
Cryptography Algorithms
Post-Quantum Cryptography
Standard Cryptography
Standard Lightweight Cryptography
First Round of the NIST (56 Alg.)
Second Round of NIST (32 Alg.)
Finalist of NIST (10 Alg.)
Cryptanalysis of LWC
Performance evaluation of LWC
LWC integrating to Standard protocols
LWC optimizations

Figure 1: Scope and objectives of this review.

C. Contribution of this study

1) Identification of published literature related to LWC algorithms and categorization of these studies into four key directions: assessment of cryptographic algorithm performance, optimization, integration of LWC, and cryptanalysis attacks on LWC.
2) This paper presents a comprehensive review of the literature on performance assessment, cryptanalysis attacks targeting various LWCs, efforts to optimize LWC, and studies focused on integrating LWC with systems and protocols.
3) Identify the current progress in hardware and software evaluation of LWC algorithms.
4) Highlighting literature that contributed to the enhancement and development of LWC and significant research utilizing these algorithms in real systems.
5) Identify research gaps that need additional study.

II. BACKGROUND

As an emerging field within cryptographic algorithms, LWC has gained prominence due to its ability to operate on devices with limited battery life, small memory capacities, or minimal physical footprint. Examples of such devices include Radio Frequency Identification (RFID) tags, sensor networks, and embedded systems [8]. The primary goal is to ensure that the machines within a restricted environment are adequately protected while maximizing resource utilization. The intent is for this cryptosystem to be strong. Although its protection properties differ from those intended for general use, they are sufficient for the target IoT systems [9]. It was challenging to develop an LWC algorithm; the developer was responsible for finding a balance between cost-effectiveness, robust security, and high performance. It is challenging to create a cryptographic algorithm that accomplishes all three of these goals [10].

NIST recently altered its security algorithms to tackle the security concerns linked to vulnerabilities in IoT communications, considering the variety of architectures and restricted energy capabilities of connected devices [11]. Furthermore, the NIST confirmed that conventional cryptographic standards for IoT devices are inappropriate for effective operation on limited devices. And consequently, NIST has called for papers to develop new LWC standards [12]. They then started a three-round standardization procedure to assess and contrast the efficacy and security of potential primitive standard cryptographic algorithms. Fifty-seven candidate algorithms were submitted to NIST for review in February 2019. In April 2019, 56 of these individuals were approved as first-round candidates. NIST selected 32 candidates for the second round after 4 months. NIST announced the ten finalists who will advance to the final phase of the selection process in March 2021: ASCON [13], Elephant [14], GIFT-COFB [15], Grain-128AEAD [16], ISAP [17], PHOTON-Beetle [18], Romulus [19], SPARKLE [20], TinyJAMBU [21], and Xoodyak [22]. NIST decided to standardize the ASCON family for LWC applications on February 7, 2023 [12] [23].

A. *Classification of finalists LWC*

There are three categories of LWC architecture: block ciphers, permutations, and stream ciphers. Block ciphers and permutation ciphers encrypt a message by partitioning it into encrypted blocks, whereas stream ciphers encrypt a message sequentially, one bit or byte at a time. The block cipher performs key scheduling, and the encryption process consistently uses the block cipher's mode of operation. Conversely, permutation is based on a key and random data-substitution processes, which enhance the capacity and speed of plaintext processing. The state is consistently encrypted during the permutation. Key scheduling is an unnecessary parameter, and design efficacy variations result in the manifestation of traits. The classification outcomes for each candidate are listed in Table I. The fundamental components of Elephant, not included in Table I, exhibit partial similarities to the permutation architecture [24].

TABLE I
Classification of the LWC Algorithms Based on the Architecture

Architecture	**Algorithms**
Block cipher	Romulus, TinyJambu, GIFT-COFB
Permutation (sponge-based)	Ascon, Xoodyak, PHOTON-Beetle, ISAP
Stream cipher	Grain-128AEAD

III. RESEARCH METHODOLOGY

To formulate a rigorous methodology, reduce bias, and ensure a selective choice of the literature, this review was conducted following the Systematic Literature Review (SLR) approach. The process stages are illustrated in Fig. 2, which enhances the reader's understanding and enables replication of these steps in future reviews. Despite a thorough search, no comprehensive analysis covering the different aspects of NIST LWC finalists exists in the existing literature. Therefore, this review is essential for compiling the key contributions related to analysis attacks on NIST LWC candidates, highlighting the most significant research on their performance, and examining the integration of LWC into the protocol.

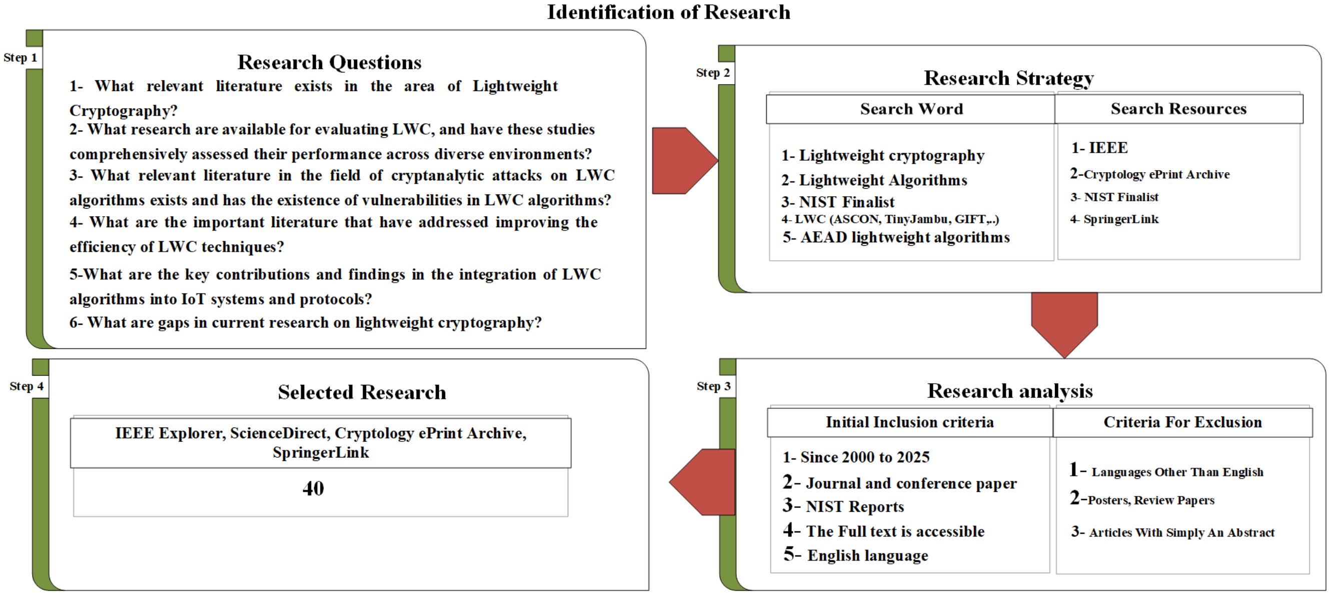
Identification of Research
Step 1
Research Questions
1- What relevant literature exists in the area of Lightweight Cryptography?
2- What research are available for evaluating LWC, and have these studies comprehensively assessed their performance across diverse environments?
3- What relevant literature in the field of cryptanalytic attacks on LWC algorithms exists and has the existence of vulnerabilities in LWC algorithms?
4- What are the important literature that have addressed improving the efficiency of LWC techniques?
5-What are the key contributions and findings in the integration of LWC algorithms into IoT systems and protocols?
6- What are gaps in current research on lightweight cryptography?
Step 2
Research Strategy
Search Word
1- Lightweight cryptography
2- Lightweight Algorithms
3- NIST Finalist
4- LWC (ASCON, TinyJambu, GIFT,..)
5- AEAD lightweight algorithms
Search Resources
1- IEEE
2-Cryptology ePrint Archive
3- NIST Finalist
4- SpringerLink
Step 3
Research analysis
Initial Inclusion criteria
1- Since 2000 to 2025
2- Journal and conference paper
3- NIST Reports
4- The Full text is accessible
5- English language
Criteria For Exclusion
1- Languages Other Than English
2-Posters, Review Papers
3- Articles With Simply An Abstract
Step 4
Selected Research
IEEE Explorer, ScienceDirect, Cryptology ePrint Archive, SpringerLink
40

Figure 2: Systematic literature review methodology.

A. Research Questions

The following research questions are the focus of this systematic literature review:

RQ1: What relevant literature exists in the area of LWC?

RQ2: What research is available to evaluate LWC, and have these studies comprehensively assessed its performance across diverse environments?

RQ3: What relevant literature exists in the field of cryptanalytic attacks on LWC algorithms, and are there vulnerabilities in LWC algorithms?

RQ4: What is the critical literature that has addressed improving the efficiency of LWC techniques?

RQ5: What are the key contributions and findings in integrating LWC algorithms into IoT systems and protocols?

RQ6: What are the gaps in current research on LWC?

B. Search Strategy

This review used a systematic methodology for article gathering, utilizing four reputable academic databases: Institute of Electrical and Electronics Engineers (IEEE) Xplore, Cryptology ePrint Archive, ScienceDirect, and SpringerLink. These significant sources were selected based on their trustworthiness, relevance to the cryptography domain, and access to high-quality peer-reviewed research.

Strategy search was used, combining broad terms like “lightweight cryptography," “lightweight algorithms," and "NIST finalist cryptography" with specific algorithm names like "ASCON," "TinyJambu," "GIFT," and "Grain-128," and refined through the use of Boolean operators (AND, OR) to optimize retrieval precision.

The inclusion criteria focused on NIST technical reports, peer-reviewed journal articles, and conference proceedings published between 2004 and 2025. Full-text access and English content were additional requirements. The research was excluded if it was published in a language other than English, had only an abstract without full text, or was classified as a non-primary source, such as a poster or a review paper. By adhering to these selection principles, the review attempted to ensure the synthesis of high-quality, relevant findings while retaining academic rigor and directly supporting the study’s focus on LWC technologies.

C. Research Analysis

Depending on the search databases, specific keywords were used in the search. This work employed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology [25], and its four-phase flow diagram was used to enhance the systematic review of the literature, as illustrated in Fig. 3. However, the 2004–2025 timeframe was used to filter the searches.

There were 2,188 papers, with all the details provided in Table II. After removing duplicate articles, off-topic articles, review papers, articles with out-of-context titles, abstract-only articles, and articles for which the full text was unavailable, 1361 articles remained in the list.

TABLE II
Distribution of Total Articles by Source Database

Source	Number of Articles	Remark
IEEE Explorer	1218	Lightweight Cryptography NIST B. Lightweight algorithms C. NIST finalist cryptography D. LWC (ASCON, TinyJambu, GIFT, Grain, . . .)
Cryptology ePrint Archive	241	
Direct Science	729	
Total Articles	**2188**	

1) Quality Assessment: To identify the primary studies, the following quality assessment questions were applied to evaluate the rigor and relevance of the selected articles.

Q1. Was the paper peer-reviewed? Yes / No.

Q2. Was there an explicit articulation of objectives? Yes / No / Partially.

Q3. Was the technique suitable for attaining the objectives? Yes / No / Partially.

Q4. Were the research context, motivation, and methodology sufficiently described? Yes / No / Partially.

Q5. Were the experimental results subjected to rigorous analysis? Yes / No / Partially.

After completing the quality assessment, the shortlisted articles were reevaluated using the following inclusion and exclusion criteria to confirm their relevance, and any studies that met one or more of the exclusion conditions were subsequently removed to produce the final set of eligible articles.

2) Inclusion Criteria:

- The article must have lightweight cryptographic algorithms as its main topic.
- The article must discuss at least one of the NIST LWC finalist algorithms.
- The article must focus on lightweight cryptography and either evaluate performance or propose enhancement methods.
- The article must address security attacks on lightweight cryptographic algorithms and/or their integration with systems and protocols.

3) Exclusion Criteria:

- The article does not address lightweight cryptography.
- The article focuses on cryptographic algorithms that are not recognized as NIST LWC finalist algorithms.
- Short articles, proposals, non-peer-reviewed technical papers, tutorials, duplicates, and off-topic.
- Short articles, proposals, technical papers, tutorials not peer-reviewed, duplicates, off-topic papers, review papers, abstract-only papers, or papers with out-of-context titles.

Finally, thoroughly assessing the eligibility of 116 papers, this paper categorized them into three groups. The first group comprises independent schemes not associated with the NIST competition. The second group includes papers based on algorithms that entered the NIST competition but did not reach the final round. After classifying the studies into three categories, 76 papers were excluded based on content review and relevance assessment, leaving 40 for the final evaluation. These 40 papers are based on algorithms that advanced to the final round of the NIST standardization process or focus on investigating lightweight ciphers in IoT applications. As shown in Fig. 3, the PRISMA framework utilized in this work consists of four steps: identification, assessment, eligibility, and inclusion.

The Institute of Reliable Embedded Systems and Communication Electronics (ivESK) at Offenburg University in Germany has provided access to all of the IEEE Xplore papers and Direct Science within the cooperation project Expanded Research, Training, and Innovation for Sustainable, Secure, and Smart Systems (ERTISSS), funded by DAAD.

D. Category A

This group comprises independent schemes not part of the NIST or CAESAR competitions. These schemes have been under development since 2004 and have continued to evolve throughout and beyond the CAESAR and NIST contests; a total of 27 fall into this category.

E. Category B

This group includes schemes that participated in the CAESAR competition, which began in 2018 and concluded with the announcement of the winners in 2023. A total of 49 articles are classified under this category, focusing on algorithms

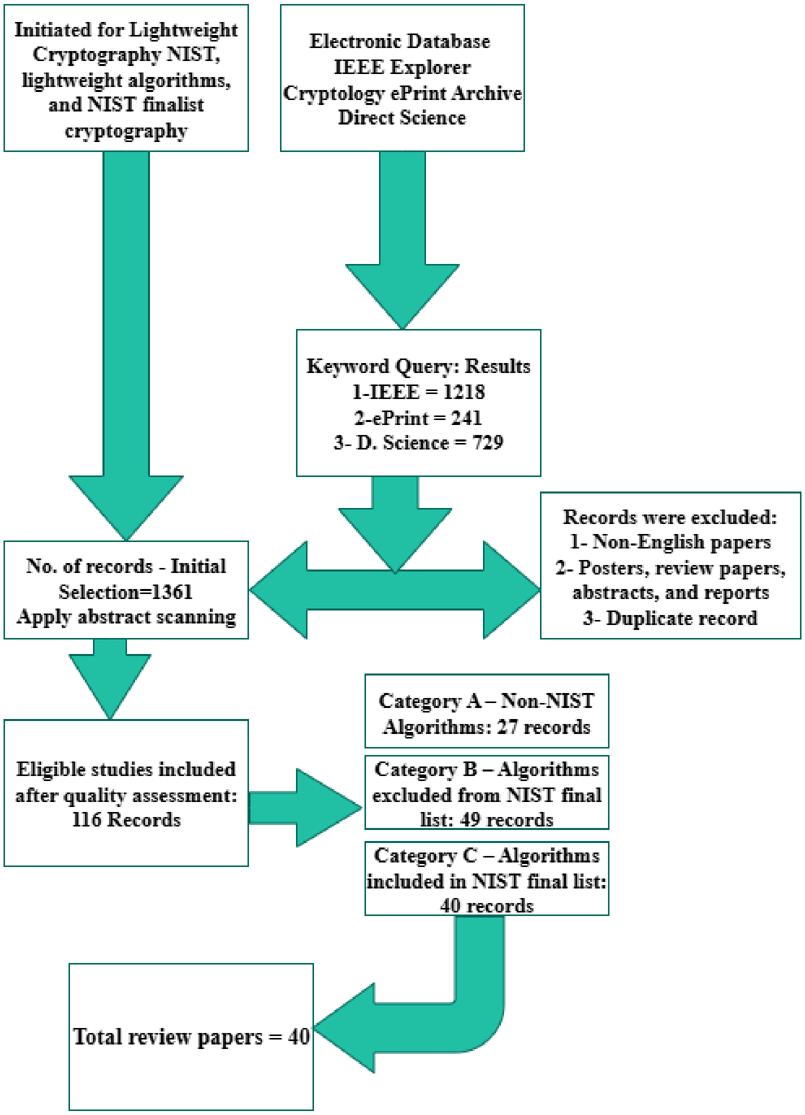
Initiated for Lightweight Cryptography NIST, lightweight algorithms, and NIST finalist cryptography
Electronic Database IEEE Explorer Cryptology ePrint Archive Direct Science
Keyword Query: Results 1-IEEE = 1218 2-ePrint = 241 3- D. Science = 729
No. of records - Initial Selection=1361 Apply abstract scanning
Records were excluded: 1- Non-English papers 2- Posters, review papers, abstracts, and reports 3- Duplicate record
Eligible studies included after quality assessment: 116 Records
Category A – Non-NIST Algorithms: 27 records
Category B – Algorithms excluded from NIST final list: 49 records
Category C – Algorithms included in NIST final list: 40 records
Total review papers = 40

Figure 3: PRISMA flow diagram for a methodical literature review analysis.

that did not advance to the final round of the NIST LWC competition. Examples include ACE, COMET, DryGASCON, ESTATE, ForkAE, Gimli, HyENA, KNOT, LOTUS-AEAD, mixFeed, Orange, Oribatida, Pyjamask, SAEAES, SANE, SLAE, Subterranean 2.0, Wage, WhirlBob, TNT, and GASCON.

F. Category C

This category comprises schemes that participated in the NIST LWC Competition, which began in 2018 and had finalists announced in 2023. A total of 40 schemes fall under this group, including references [26-66]. Since 2019, research on LWC has increased dramatically, with the number of publications doubling over the previous years. This increase can be attributed to two primary factors: the rapid expansion of IoT applications and their extension into new areas such as Industrial IoT, and the launch of the NIST Lightweight Cryptographic Standardization Project in 2019, which encouraged researchers to develop more efficient, lightweight algorithms. As a result, more than 750 studies were published between 2023 and 2024 alone. Furthermore, the recent release of the finalist algorithms sparked an entirely novel phase of research into their performance and resilience to various cipher attacks. Fig. 4, Fig. 5, and Fig. 6 illustrate this trend and its significant impact on LWC in the cryptographic field. The NIST has resolved the ongoing debate regarding evaluating and classifying new and improved algorithms compared to previous ones. It finalized a list of ten algorithms selected from a competition, officially naming them the "Lightweight Cryptography." This decision enables researchers to identify light algorithms and quickly explore new research opportunities. The development of finalist LWC increased significantly from 2019 to 2025. There has been a growing interest in LWC, which has become a key component in many systems and protocols designed to secure data, particularly in IoT applications. This interest stems from the need for lightweight, efficient security solutions for resource-constrained devices.

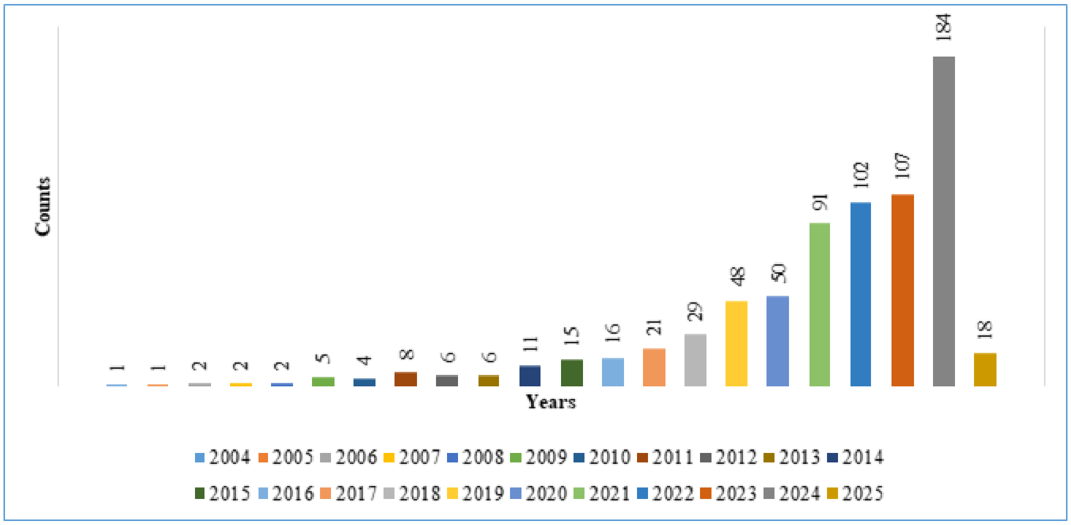

Figure 4: Number of research publications on LWC per year in IEEE Xplore.

IV. PRESENTATION OF LWC APPROACHES

This part outlines the primary contributions of the selected approaches to LWC. The first section refers to research that facilitated the assessment and analysis of LWC algorithms. The second section focuses on research that analyzes attacks on LWC algorithms. The third section outlines the main contributions to optimizing the performance of LWC. The final section emphasizes the principal studies that investigate incorporating lightweight algorithms into IoT protocols.

A. LWC Algorithm Software and Hardware Performance Comparison

Numerous researchers have evaluated the performance of the finalist LWC algorithms across different platforms. In [26], the researchers presented a performance evaluation of ASCON, focusing on two variants, Ascon-128 and Ascon-128a; this

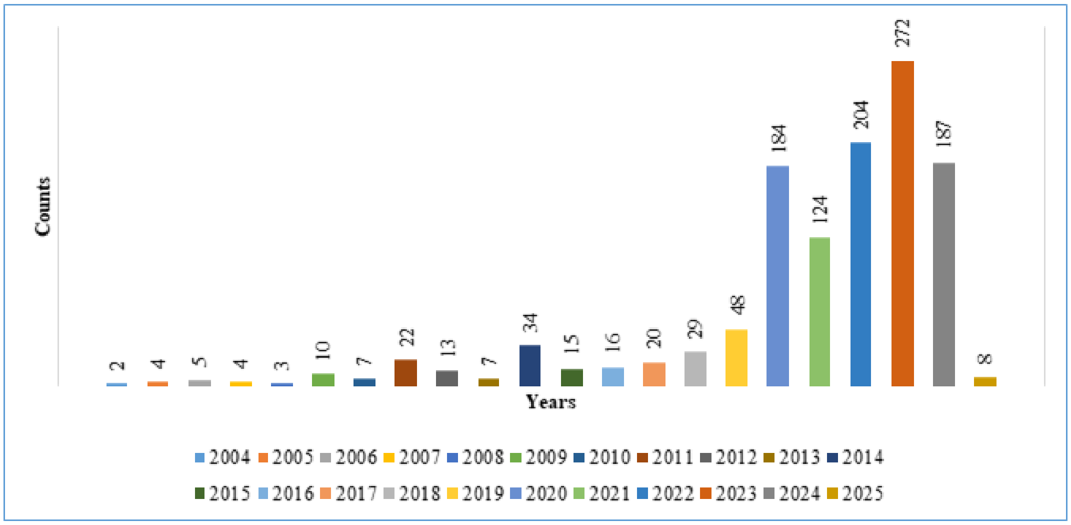

Figure 5: Number of research publications on LWC per year in ScienceDirect.

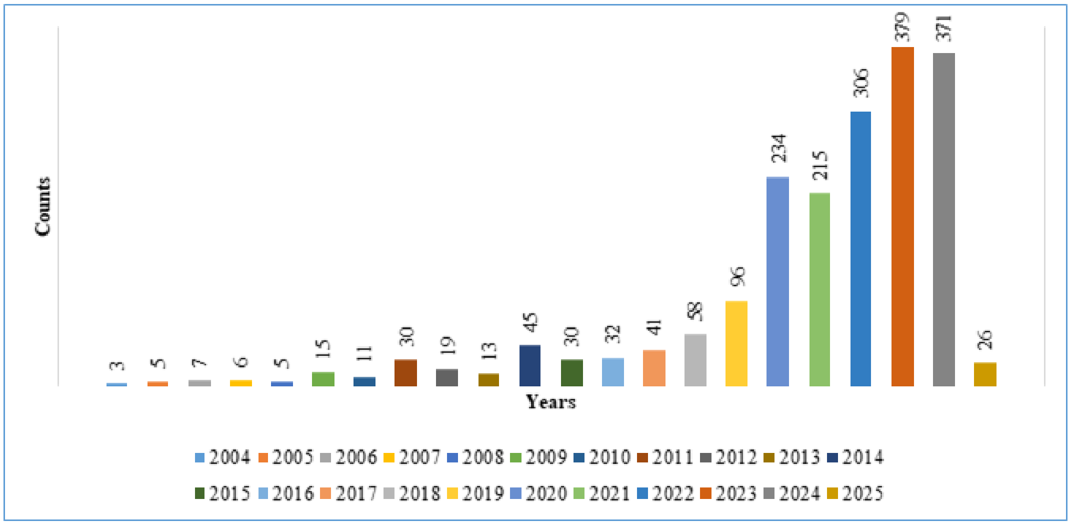

Figure 6: Total and annual research publications on LWC.

work assesses the hardware implementation of ASCON, an LWC standard chosen by NIST, on 7-series FPGA devices. Using a finite-state machine-based and iterative design-level approach, the study achieves noteworthy performance metrics, including frequency ranges of up to 335 MHz and power consumption of 219 to 239 mW across various FPGA devices. In [27], the authors used an Arduino to evaluate the LWC block ciphers GIFT-COFB, Romulus, and TinyJAMBU. The results showed that TinyJAMBU performed better than the others in terms of execution time and power consumption, which makes it a good option for IoT devices with limited resources. The authors in [28] conducted an energy evaluation of the hardware performance of the LWC candidates. The study used Application-Specific Integrated Circuit (ASIC) synthesis over 22nm

Complementary Metal–Oxide–Semiconductor (CMOS) technology. It focused on metrics like energy efficiency (bit/joule), throughput, and area, which are crucial for resource-constrained devices like IoT and Unmanned Aerial Vehicles (UAVs). The evaluation of NIST LWC finalists revealed significant differences in energy efficiency. Algorithms such as ASCON, TinyJambu, and Xoodyak showed 10–25 times higher energy efficiency than other algorithms while time-processing the same amount of data. In [29], the researcheres present the initial depth-optimized quantum-circuit solution for ASCON, a symmetric-key cipher specified by NIST. The suggested implementation's modest Toffoli depth and manageable qubit count make a practical post-quantum security evaluation possible. The study in [30] analyzes NIST LWC standards finalists on ATmega 128 and ARM Cortex-M3 microcontrollers for embedded device RAM optimization. In [31], the author analyzed the hardware implementations of ten NIST LWC standard candidates synthesized using TSMC 65nm and FDSOI 28nm technologies. In [32], the authors evaluate NIST's LWC algorithm submissions ASCON, DRYGASCON, and SHAMASH for cryptanalysis security; the results found probability one subspace trails and shortened differentials for Shwamm, and improved the data and time execution of differential-linear assaults on ASCON. Table III summarizes these studies, the evaluation methods, and the key findings. In summary, ASCON and TinyJambu dominate in software-based and hardware-efficient LWC algorithms. The reviewed research indicates an increasing interest in assessing lightweight algorithms in recent years, underscoring their significance.

TABLE III
Performance Metrics and Key Findings of Research Papers Investigating LWC Algorithms

Ref.	**ALG.**	**ARCH.**	**DES.**	**TH.**	**ET.**	**M**	**U**	**SE.**	**Main Findings**
[26]	ASCON	FPGA	Hardware	✓	✓	×	✓	✓	The findings show that Ascon performance on Kintex-7 FPGA devices operates at the highest frequency, and the design is generally suitable for a wide range of applications, including mobile technologies and embedded systems.
[27]	Gift, Romulus, TinyJambu	Arduino	Software	✓	✓	✓	✓	×	TinyJAMBU demonstrated the best overall performance in a realistic operating environment.
[28]	NIST Finalist Alg.	FPGA	Hardware	✓	✓	×	×	×	The results demonstrated that Xoodyak performs best in continuous long message scenarios, while TinyJambu is the most energy-efficient algorithm for bursting short messages.
[29]	ASCON	Quantum Circuit	Theoretical	×	×	×	×	×	The study concludes that ASCON's post-quantum security is Level 1, similar to AES-128.
[30]	NIST Finalist	ATmega & ARM	Software	×	✓	✓	✓	×	TinyJAMBU-128 used the least RAM of all AEAD schemes, making it appropriate for resource-constrained IoT applications.
[31]	NIST Finalist	FPGA	Hardware	✓	×	✓	✓	×	Optimizing specific applications is crucial because candidate performance varies significantly across different use cases. Some strategies are more efficient in particular contexts.
[32]	ASCON	×	Theoretical	×	×	×	×	✓	Although ASCON and DRYGASCON share architectural similarities, SHAMASH's improvements make it a distinct cipher, justifying its exclusion from the NIST competition.

**The table employs the following abbreviations: REF. (Reference), ALG. (Algorithm), ARCH. (Architecture), DES. (Design), TH. (Throughput), M. (Memory), ET. (Execution Time), FAM. (Algorithm Family), U. (CPU Utilization), and SE. (Security Evaluation).*

The comparative evaluation is shown in Fig. 7, derived from four related experimental studies [27][28][30][31], with each metric standardized to (0,1) to harmonize the measurement range across all evaluation matrices. This normalization made sure that different parameters could be compared fairly and evenly. Fig. 7 shows the overall computational performance of each lightweight algorithm, combining normalized results for throughput, energy efficiency, and latency. It indicates that Photon-Beetle, Xoodyak, and ASCON are at the outer edges of the radar plot in the throughput dimension. This means they can process data more effectively and achieve higher throughput. These algorithms work well for encrypting large messages and sending them quickly. ISAP, Elephant, and Grain-128AEAD appear closer to the center, indicating poorer throughput performance and thus limited applicability in latency-critical IoT scenarios. TinyJambu dominates the corresponding axis in terms of energy efficiency, with a normalized value of 1.0, indicating exceptional power optimization and confirming its suitability for energy-constrained devices like sensor nodes. ASCON and Xoodyak demonstrate a balanced trade-off between speed and efficiency, whereas ISAP and Grain128-AEAD rank lowest in this dimension, implying higher power consumption per operation. TinyJambu, Xoodyak, ASCON, and Schwaemm have the highest radial extension (1.0 normalized) on the latency axis, demonstrating responsiveness in time-sensitive communication. In contrast, Elephant contracts sharply toward the center, indicating excessive processing delay and poor suitability for real-time tasks.

Overall, Fig. 7 proves that TinyJambu, ASCON, and Xoodyak are in the optimal performance range, combining high throughput, strong energy efficiency, and low latency. Photon-Beetle remains the fastest, but at a higher energy cost, whereas Elephant and Grain perform poorly in all three dimensions. Elephant and Grain, on the other hand, don't do well in any of the three areas.

Additionally, Fig. 7 demonstrates the significant utilization of system resources, as shown by the normalized values of ROM size, Stack usage, and CPU utilization. TinyJambu, Xoodyak, and GIFT have the highest normalized values on the ROM Size axis (close to 1.0), indicating they use very little memory and are easy to implement. Grain near the center has the highest stack requirements, which can be a problem in embedded environments that need to do more than one thing at a time or are driven by interrupts. In CPU utilization, lower normalized values indicate more efficient processing. GIFT, TinyJambu, and ISAP have the least CPU load. On the other hand, Photon-Beetle and Grain are close to the center, which means that they need a lot of CPU power and can't run many tasks at once. Fig. 7 shows the balance between ease of implementation and the additional processing power required. TinyJambu is still the best at both ROM and stack efficiency, but GIFT is the best at CPU utilization. On the other hand, Photon-Beetle needs more resources, which might make it challenging to use in embedded systems with very little memory or power.

B. Cryptanalysis Attack on LWC Algorithms

Numerous types of cryptanalysis attacks have been published in the literature. These studies cover various types of analysis, including differential, side-channel, and fault attacks. Cryptanalysis uses a variety of attacks and decoding methods to find algorithmic weaknesses. This review has classified researches based on the algorithms' architectures. Fig. 8 illustrates the classification of attacks on LWC algorithms. Table IV summarizes the main contributions. In [33], the authors presented notable improvements in preimage and collision attacks targeting the Ascon family of cryptographic algorithms. In [34], the best-known time complexity for attacks on the 26 rounds of the GIFT-64 was achieved using an enhanced rectangular-key recovery attack on the lightweight block cipher. In [35], the researchers proposed a conditional cube strategy for Xoodyak

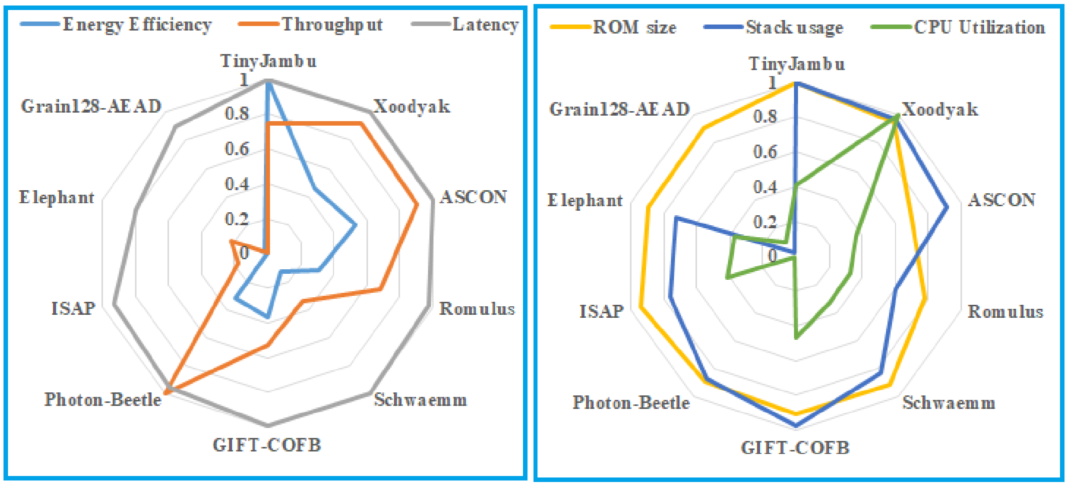

Figure 7: Comprehensive Efficiency Evaluation of LWC.

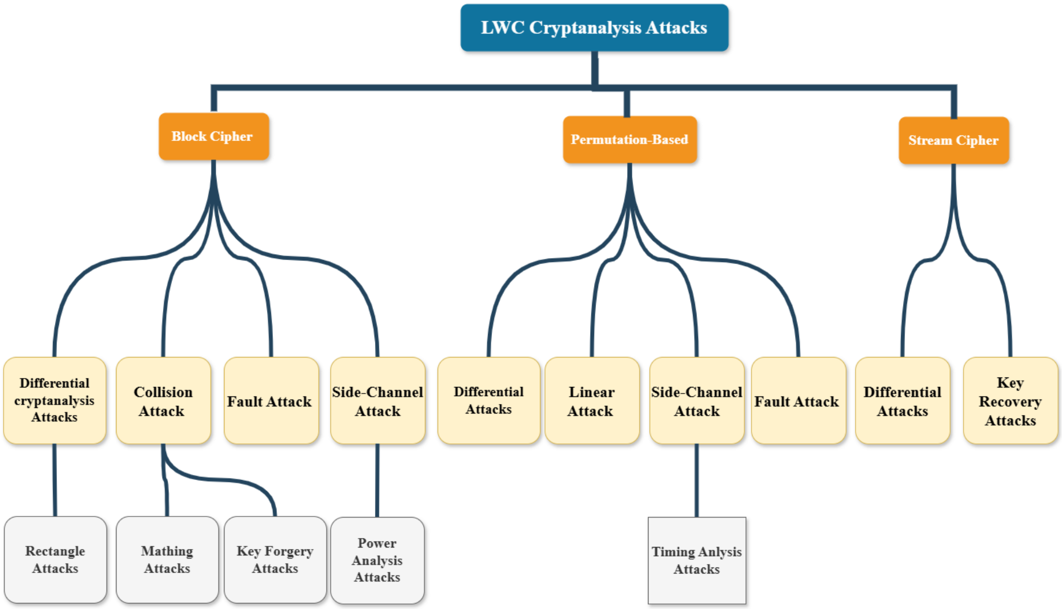

Figure 8: Classification of Attacks on LWC.

that recovers the key in 6 and 7 rounds, respectively. In [36], the authors introduced Ascon's tree-based trail search tool for quickly constructing and expanding differential and linear trails. This approach enhances Differential Probability (DP) and squared correlation (C^2) bounds, obtaining tighter limits for 3-round trails and exceeding previous limits for 6 and 12 rounds. Effective related-key forgery attacks on the revised TinyJAMBU scheme with 192- and 256-bit keys are presented. The cyclic structure of the keyed permutation enables high-probability differential assaults, resulting in forging complexity. The cyclic key schedule and insufficient related key attack protections during initialization are the causes of the key forgery vulnerability. Implementing a key schedule or doubling the rounds in P^b and P^a is necessary for mitigation. The 192-bit and 256-bit versions' extra key processing using P^a was one of the fixes suggested by the authors after they confirmed the attacks.

In [38], the researchers assessed the Xoodoo cryptographic permutation's cryptanalysis resistance; they improve methods for tighter bounds on its differential and linear trails, address existing limitations, and demonstrate the effectiveness of their optimized trail extension techniques by setting new minimum weights for 4, 6, and 12 rounds. In [39], a novel side-channel key retrieval attack on Elephant, an LWC contender for NIST, using Correlation Power Analysis (CPA) on an ARM Cortex-M4 microcontroller to recover the secret key in one minute with only 30 power traces. In [40], the authors used realistic attack examples to show that Romulus-M, a NIST LWC project winner, has tight security boundaries for various parameters. In [41], the authors proposed improvements to Cellular Automata (CA) for ASCON and GIMLI to make them more resistant to fault attacks and demonstrate their security against the discovered vulnerabilities. In [42], they critically evaluate two finalists, Photon-Beetle and GIFT-COFB, and identify weaknesses that contradict their security claims. In particular, assaults with greater success probabilities than documented are shown. The researcher in [43] studied a lightweight block cipher, COFB mode, against forgery and privacy attacks, but it is limited by the number of forgery attempts. The investigation shows that COFB behaves like an Authenticated Encryption with Associated Data (AEAD) with a 64-bit tag despite outputting a 128-bit tag. In [44], the authors present advancements in the cryptanalysis of the Xoodyak lightweight algorithm and also investigate the Xoodyak permutation, which underlies the NIST standardization contender Xoodyak and creates a zero-sum distinguisher for 12-round Xoodyak, but it does not attack it. The authors in [45] present multiple byte-based differential fault attack techniques for the lightweight cipher GIFT, targeted for resource-constrained environments such as the IoT. Experimental results demonstrate that the models require 79 and 16-byte errors to retrieve the master key, compared to 53.44 and 12.42 theoretically.

In [46], the authors introduced misuse-free nonce-key-recovery and distinguishing attacks on the seven-round Ascon authenticated encryption scheme, employing partial polynomial multiplication to efficiently recover superpolies. The key recovery attack exhibits a time complexity of roughly 2^{123} and necessitates a memory requirement of 2^{101} bits while also uncovering new cube distinguishers for Ascon within the AEAD context. In [47], the authors introduced the first extensive hardware implementations of the ASCON lightweight cipher, including unsecured and protected versions against fault attacks and side-channel attacks, with ASIC and FPGA benchmarks. They demonstrated that limited implementations for side-channel protection and triplication for fault protection can be engaged separately, allowing hardware design flexibility.

In [48], the authors presented a chosen-plaintext attack on the GIFT-COFB lightweight encryption algorithm that exploits the hardware implementation of the S-box nonlinearity to recover the secret key. The analysis indicates that GIFT-COFB's efficient design may be vulnerable to the suggested attack, which requires only three nonce-tag pairs to recover the secret key. A novel method for recovering super policies was proposed in [49], who used it to recover the 192-round Grain-128AEAD secret key using 2127 queries. After 192 rounds, the attacker is assumed to have access to the pre-output bits.

In [50], the authors introduced a strategy of simply re-entering the key into the state, which may not be sufficient to ensure its confidentiality; they show that key recovery is still possible under various circumstances even after applying specific design modifications.

To demonstrate the first third-party cryptanalysis of Elephant Delirium and to increase the effectiveness of attacks on Kravatte, the authors in [51] proposed an interpolation attack that uses the Moebius Transform to efficiently analyze round-reduced versions of the Elephant ciphers. As demonstrated through multiple attack scenarios, reintroducing the key into Grain-128AEAD's internal state does not completely prevent key recovery. According to the results, other techniques might be required to improve security, such as returning the key to the NFSR state right after initialization. In [52], the authors outlined a two-step method for finding beneficial distinguishers in block ciphers, specifically applied to GIFT-128. It focuses on differential and linear trails that can be extended with little key involvement. The authors effectively demonstrated a new strategy by outperforming prior results, achieving 27-round differential and 22-round linear hull attacks on GIFT-128. The authors in [53] analyze Grain-128AEAD LWC authenticated encryption stream cipher's differential fault vulnerability. The results show that bit-flipping and probabilistic random fault attacks can recover the cipher's initial state. Still, the stochastic random fault attack with moderate control is the most practical, as it requires fewer fault injections and lower data complexity. Important findings: Differential fault attacks can compromise Grain-128AEAD, and the stochastic-random fault attack recovers the state most efficiently. In resource-constrained environments, LWC algorithms must be tested for side-channel attacks.

C. Optimizing algorithms

In [54], a new approach was introduced to optimize Ascon's algorithm for improved speed on Reduced Instruction Set Computer (RISC-V), an open-source architecture. Ascon relies on 320-bit state and permutation functions to provide security in resource-constrained devices. The optimization efforts aimed at achieving the highest possible speed while using as few registers as possible, considering the unique challenges of the RISC-V architecture. Some of the most critical changes were resolving endianness issues, adding bit-slicing techniques to the substitution layer, and improving the linear diffusion layer for better performance despite RISC-V's built-in limitations. Among the notable contributions of this work was the development of an optimized instruction sequence for S-box computation. Implementing bit slicing cuts the number of operations needed for S-box processing from 44 to 17. A combining technique made it much easier to work with 64-bit state words. In [55], new approaches to optimizing ASCON are proposed. Researchers improved the operational frequency of the permutation function and efficiency with a Chisel-based FPGA design. Using multi-clock strategies and pipelining, they reached a 233.3 MHz operational frequency, improving resource efficiency. The design optimizes processing and throughput speed by dividing permutations into two stages: the addition constant and the substitution stage. An additional diffusion layer optimizes the algorithm by enabling each stage to operate at its maximum clock rate, thereby boosting the overall throughput. This novel architecture improves performance and sets a new standard for LWC in constrained environments. In the field of block ciphers, the authors [56] presented a study of implementations of the lightweight TinyJAMBU cipher using shift register parallelization to reduce dynamic power by over 30% while maintaining resource efficiency for low-power IoT applications. The author in [57] executes the Schwaemm256 algorithm from the SPARKLE permutation family to make data transmission more secure in smart lock systems that use the ESP-NOW communication protocol. They conducted

TABLE IV
Summary of cryptanalysis attacks on LWC algorithms

Ref.	algorithms	Attacks analysis	Main Findings
[33]	ASCON	Collision attacks	Enhanced Preimage Attacks: Using a more sophisticated guessing technique, the authors improved the preimage attack on 2-round Ascon-XOF, reaching a suitable complexity. Additionally, they expanded their approach to three rounds and automated the guessing process using a Mixed Integer Linear Programming (MILP) model. For various initialization vector circumstances
[34]	Gift	Rectangle attack	1. By pointing out flaws in earlier assaults and suggesting a method to balance the time complexity of various attack phases, the authors reassess the rectangle assault on GIFT-64 in a related-key scenario. 2. By extending the research to GIFT-128, the study shows a decrease in attack complexity, which advances our knowledge of the GIFT encryption family's security.
[35]	Xoodyak	A cube Attacks	1. First successful attack on 7-round Xoodyak expands cryptanalysis for LWC algorithm. 2. Using the conditional cube attack strategy by importing cube variables during data absorption increases assault freedom and effectiveness.
[36]	ASCON	Differential Attacks	1. The Ascon TrailTool was created as an exclusive instrument that uses innovative tree traversal and trail extension algorithms to explore more significant trail regions at lower computational costs. 2. Improved upper limits for differential and linear trails in Ascon.
[37]	TinyJAMBU	Keys forging attacks	1. An incremental related-key differential feature for TinyJAMBU mode enables forging attacks with controllable time and data complexity. 2. TinyJAMBU design weaknesses, notably in the 128-bit variant, require increased related-key attack protection.
[38]	Xoodyak	Differential & linear Attacks	1. Effectively uses optimization techniques to improve trail search efficiency, overcoming computational bottlenecks and establishing tighter constraints for Xoodoo's differential and linear trails. 2. The study validates tight boundaries for 4-round trials and expands them for 6 and 12 rounds, improving our understanding of Xoodoo's cryptographic strength against differential and linear assaults.
[39]	Elephant	Key-Recovery Attack	1. The study found that by employing 35 power traces, the attack can recover the entire secret key with over 90% success rate and can be applied to different Elephant cipher variations. 2. Experimental results show that the attack is feasible and can be implemented on standard hardware, raising concerns regarding the LWC method's side-channel security.
[40]	Romulus	Matching Attacks	1. Prove that Romulus-M achieves tight security constraints for privacy and authenticity, confirming optimal attack success probabilities. 2. Attackers exploit Romulus-M's structure to attain success probabilities close to the security bounds, verifying their tightness.
[41]	ASCON	Fault Attacks	1. The authors found that ASCON and GIMLI are vulnerable to fault attacks, which can impair their security in practical implementations. 2. Incorporating cellular automata into the encryption process makes SIFA and SSFA ineffective, making attacks more difficult.
[42]	GIFT-COFB & Photon-Beetle	Privacy Attacks	1. GIFT-COFB's security constraints are contradicted by an attack that violates privacy with fewer queries than required. 2. Photon-Beetle's authentication guarantees are invalidated by a simple counterfeit attack that exploits the lack of encryption query contribution without basic inquiries.
[43]	GIFT_COFB	Chosen Ciphertext Attacks	1. The data protection of GIFT_COFB is significantly affected by the number of forgery attempts, with a probability of success. 2. The analysis contradicts earlier security proofs and shows a security gap between proven results and realistic attacks, underlining the importance of nonce sizes and attack techniques in lightweight encryption.
[44]	Xoodyak	Algebraic Attacks	The article shows that managing variable propagation and building efficient linear equation systems can significantly lower the time complexity of preimage attacks. According to the study, the effectiveness of cryptoanalysis should be assessed by the time required to solve linear equation systems.
[45]	GIFT	Differential Fault Attack	1- This study shows that byte-based differential fault attack frameworks are more efficient, reducing the number of faults needed for key retrieval. 2- The findings help develop better, more secure cryptographic systems for IoT devices by revealing GIFT algorithm flaws and suggesting fault-tolerant mechanism enhancements.
[46]	ASCON	Cube attack	The most effective attack requires 2^{64} data and 2^{101} bits of memory to recover the 128-bit secret key with a time complexity of roughly 2^{123} 7-round Ascon permutations.
[47]	ASCON	Side Channel & Fault Attacks	With side-channel attack safeguards, ASCON requires 12.57 times the space of the unprotected ASIC version on both ASIC and FPGA platforms. It also shows that well-designed hardware implementations may secure the ASCON cipher against physical attacks, enabling its use in resource-constrained IoT devices.
[48]	GIFT-COFB	Chosen-plaintext attacks	Chosen-plaintext attacks can deduce the master key from GIFT-COFBs—round partial unrolled design's encryption outputs with minimal nonce-tag pairings. Analyzing GIFT's S-box structure allows the attacker to uniquely discover key cells by exploiting the encryption's internals.
[49]	Grain128	Recovering Key attacks	Reintroducing the encryption key into the internal state does not prevent key retrieval under various attack scenarios. It shows how to recover the encryption key from the internal state, contradicting the design's security claim.
[50]	Elephant	Recovering Key attacks	The results indicate that the interpolation attack can analyze ciphers like Elephant-Delirium, Kravatte, and Xoodyak with minimal algebraic degree update functions.
[51]	Elephant	Interpolation Attacks	This paper demonstrates the effectiveness of interpolation attacks on elephant algorithms when combined with the Moebius Transform and linearization, and highlights possible vulnerabilities in the LWC architecture.
[52]	GIFT-COFB	Differential attack	Applying a new strategy to GIFT-128 enabled significant cryptanalytic accomplishments, including the first 27-round D-A and a 22-round linear attack. These results show how practical the suggested approach is, as it outperforms earlier cryptanalysis attempts on GIFT-128 and exposes its possible flaws.
[53]	Grain128	Differential fault attacks	The deterministic theory of stochastic fault attack with limited control is the most useful, involving fewer fault injections and information complexity than the other models. All attacks recover the cipher's initial state.

their experiment on ESP32 devices with an average runtime of 1.556 seconds and 72.9% free memory. The study in [58] suggested better lightweight algorithms called ALIT-Hash and TJUILIK-Hash. These are two lightweight hash functions based on PHOTON-Beetle, designed for the IoT and for protecting data integrity with minimal computing power. They are resistant to cryptanalysis and perform well on low-power microcontrollers. ALIT-Hash and TJUILIK-Hash work well in IoT environments with limited resources. They are resistant to differential and linear cryptanalysis attacks and can run in 0.746 microseconds on low-power microcontrollers. A study in [59] tested 10 algorithms chosen by NIST to see how well they protect data privacy and integrity on devices with limited resources. They examined the cryptographic properties of the confusion layer. The tested S-boxes all meet the basic cryptographic requirements. However, looking into how well they protect against more advanced cryptographic threats will be necessary as attack strategies change. This implies a need for further research to enhance their safety. Key findings: To combat new cryptographic attacks, the study recommends analyzing S-box performance under linear, differential, and side-channel attacks. Future research should suggest developing S-boxes that balance linear and differential cryptographic strengths with side-channel resistance.

D. Integrating LWC into protocols

This section will focus on published research on LWC and its contributions to security-enhancing protocols. In [60], the authors proposed an IoT authentication protocol that uses the Ascon cryptographic family, recently standardized by NIST, to improve resistance to impersonation and confidentiality of data transmission. In [61], the authors introduced a vision paper that explores the integration of LWC algorithms, specifically ASCON and Grain128-AEAD, with the MQTT protocol to enhance security in Internet of Things (IoT) networks, emphasizing the importance of confidentiality, data integrity, and efficiency in resource-constrained environments. The study concluded that while encryption increases IoT data processing time, algorithms improve security while maintaining efficiency, with ASCON outperforming Grain128-AEAD. In [62], the authors proposed a novel security design for the Internet of Vehicles (IoV) using lightweight encryption algorithms, such as ASCON and GIFT-COFB, to improve data integrity and communication security in Message Queuing Telemetry Transport (MQTT) based IoV systems. Due to their vulnerability to cyberattacks, IoV networks require robust security measures, and the proposed cryptographic solutions can securely exchange data while accommodating the limited processing capabilities of IoT devices. In [63], the authors discussed the IoV and its security and privacy issues. They propose a new secure data transfer approach using MQTT and LWC methods, such as ASCON and GIFT-COFB. It emphasizes the importance of robust security in IoV systems and lightweight encryption approaches that leverage IoT devices' despite their limited capabilities to protect data integrity and confidentiality during communication. In [64], the authors offered a low-cost IoT communication architecture using Raspberry Pi Pico microcontrollers, LoRa RYLR896 radio modules, and ASCON-based encryption to improve data transfer for resource-constrained IoT devices. In [65], the authors proposed a framework to evaluate the ESP32 microcontroller and the MQTT protocol to secure kart telemetry data, including steering angle and throttle position, using the GIFT-COFB LWC algorithm. Encryption decreased throughput and increased delay and jitter, and the GIFT effectively protects data, but it takes longer to execute. The major conclusions are that GIFT-COFB algorithm improves the security of kart telemetry data but increases processing time and reduces data throughput. Despite these issues, encryption maintains quality of service standards, protects data, and prevents unauthorized access. T. Al-Hasan et al. [66] tested ASCON, TinyJambu, and Xoodyak on a Raspberry Pico W microcontroller for IoT device security, focusing on energy efficiency. The throughput of these algorithms is measured while transmitting sensor data over MQTT. ASCON's high cryptographic strength resulted in lower encryption and decryption throughput rates of 1.6 and 1.35 MBps, respectively, while TinyJambu was the most efficient at 1.8 and 2.1 MBps. Despite its larger code footprint, Xoodyak performed moderately at 1.6 and 1.3 MBps. All three algorithms secured end-to-end MQTT communication, demonstrating their potential for securing resource-constrained devices. The findings suggest that LWC algorithms can improve energy effectiveness and environmental sustainability in applications for the Internet of Things, which paved the way for hardware acceleration research. Table V summarizes the primary research on integrating LWC into protocols.

V. RESEARCH GAPS

This section provides an overview of the research gaps regarding LWC that must be addressed in future research.

First, the approaches presented in Section IV are examined to evaluate LWC performance. Despite the significant number of research studies analyzing the performance of lightweight encryption algorithms, considerable variation in their evaluation leads to inconsistent outcomes. Some of these studies fail to cover many aspects of analysis and lack precise results. Many cryptographic analysis studies focus on algorithms like GIFT and ASCON. However, a comprehensive analysis encompassing all the finalist algorithms is lacking. This gap is crucial and should attract the attention of researchers in the future, as these algorithms were designed and selected to serve a wide range of diverse applications. A comprehensive, unified evaluation framework for LWC algorithms is needed, encompassing both software and hardware-based implementations and employing consistent performance metrics to ensure fair, comparable assessment.

Second, Section IV.B covers attack analysis and security assessment of lightweight encryption algorithms. These studies fail to provide thorough evaluations or in-depth analyses of how resistant the algorithms are to sophisticated adversarial tactics. Due to the lack of research in this area, targeted studies are needed to systematically assess attack resilience across various algorithmic architectures. The scarcity of security research on Xoodyak, ISAP, Photon, TinyJambu, and Romulus is notable, as no results demonstrate a clear security evaluation of these algorithms. A standardized framework should be developed for assessing the resistance of lightweight cryptography (LWC) algorithms to fault-analysis attacks. The framework defines uniform parameters for fault-injection scenarios (number of samples, injection-timing accuracy, and fault models), attack performance metrics (samples-to-key, success rate, and computational cost), and countermeasure evaluation (masking, redundancy, and glitch detection). To ensure fair and reproducible comparisons, it applies common fault models across multiple algorithms, including ASCON, GIFT, PHOTON-BEETLE, SCHWAEMM, and Grain-128AEAD, among others.

Third, the researchers' security claims remain unchallenged by existing security analyses. The most effective key recovery attacks documented thus far include targeting 7 out of 12 rounds for ASCON [45], 8 out of 18 rounds for Elephant [49], 192 out of 512 rounds for Grain-128AEAD [49], and 27 out of 40 rounds for GIFT-COFB [51]. This emphasizes the need for more research covering all lightweight encryption algorithms and examining different attack vectors.

Fourth, Section IV.C highlights significant advancements in the optimization of lightweight encryption algorithms. However, despite their significance, this field has a noticeable dearth of research. These algorithms remain in the early stages of development, and their performance has not yet been significantly enhanced for deployment across various settings and

TABLE V
Summaries of Integrating LWC into Protocols

Ref.	Algorithm	Protocol	Contribution	Findings
[60]	ASCON	new authentication protocol	Improved resistance to various attacks	The new IoT authentication protocol is more secure than others, reducing the risk of key compromise and replay attacks. The protocol provides secure message transfer across devices, so even if a single session key is compromised, the others remain safe, making it a viable solution for resource-constrained IoT environments.
[61]	ASCON, Grain128	MQTT	It significantly improves the security of IoT data transmission.	ASCON and Grain128-AEAD combined with the MQTT protocol improve IoT security, but data processing is delayed. ASCON processes faster than Grain128-AEAD, so while both algorithms are adequate for IoT systems, ASCON may be better for performance-critical applications.
[62]	ASCON, GIFT	MQTT	Secure IoV protocols using ASCON, GIFT-COFB.	Experimental research demonstrates that the ASCON and GIFT-COFB algorithms can efficiently encrypt and decrypt up to 10 gigabytes of data in under 1300 milliseconds, making them ideal for resource-constrained IoT applications.
[63]	ASCON and GIFT	MQTT in IoV	Secure IoV-based LWC with data confidentiality and authentication	An experimental study demonstrates that the ASCON and GIFT-COFB algorithms are efficient encryption and decryption algorithms suitable for real-time IoV applications, achieving adequate performance metrics for data sizes typical of such contexts.
[64]	ASCON	LoRa RYLR896	Provide high SNR, RSSI, and power consumption.	For low-powered IoT devices, ASCON surpasses AES in energy consumption and memory utilization, prolonging battery life and improving data speeds.
[65]	GIFT-COFB	MQTT	The proposed system protects data confidentiality.	Quality-of-service analysis showed that encryption reduced throughput and increased time delay and jitter, while maintaining an excellent packet loss rate, highlighting the trade-off between data security and transmission efficiency.
[66]	ASCON, TinyJambu, and Xoodyak	MQTT	LWC algorithms secured end-to-end MQTT communication	LWC algorithms can improve energy effectiveness and environmental sustainability in applications for the Internet of Things

devices. Current studies have not led to considerable improvements in their efficacy. It is crucial to make two separately optimized versions of each algorithm: one for software and one for hardware, and future studies should test how well they work on different devices. It is also essential to enhance the operational efficiency of certain algorithms. In the TinyJambu algorithm, for instance, Linear Feedback Shift Register (LFSR) operation could be performed concurrently with the plain permutation process when working with large datasets. In the same way, the SPARKLE algorithm could combine and execute multiple permutation operations at the same time to improve overall efficiency.

Fifth, the integration and utilization of LWC algorithms in IoT applications and their uses in security protocols such as IPsec, TLS, and Secure MQTT (SMQTT) are essential elements shaping the future of cybersecurity. Significant contributions to this field are highlighted in section IV.C, especially the integration of network protocols and LWC techniques. Although most prior studies have focused on integrating LWC algorithms into the MQTT protocol to ensure information confidentiality and reliability, further investigation is still required. These algorithms are highly effective and adaptable at delivering essential security services, making them ideal candidates for integration into diverse protocols and systems. A top research priority is the comprehensive assessment of countermeasures, including masking, redundancy, and glitch detection. To ensure that algorithms meet essential security requirements, standardized fault models should be applied across diverse implementations. Furthermore, critical research gaps must be addressed by evaluating the performance of emerging algorithms when integrated into real-world systems and communication protocols. Finally, the fifth research gap highlights the importance of optimization techniques and performance enhancements to improve the efficiency and practical usability of lightweight cryptographic implementations.

VI. CONCLUSION

This final section summarizes the work at hand. Following the research questions presented in Section III.A, a PRISMA methodology was applied. Relevant research articles were systematically selected based on their alignment with the study scope. Fig. 2 and 3 illustrate the systematic methodology, including the sequential steps and keywords. Fig. 6 shows the annual publication volume in this domain, revealing a significant increase in academic articles on LWC algorithms in recent years.

The first research question is crucial because it clarifies the core objective and direction of scientific investigations in the lightweight cryptography domain. The analysis of 116 papers shows that about 70% of the studies focus on security, cryptanalysis, and algorithm evaluation, as researchers aim to identify potential weaknesses and vulnerabilities in newly proposed LWC algorithms [26–53]. In contrast, fewer studies focus on algorithm design and optimization, system integration, and application-oriented evaluations, despite the fact that some algorithms have passed the NIST requirements are strong and still receive limited research attention.

RQ-2 was addressed by summarizing the findings using the approaches selected in Section IV.A. Table IV summarizes the research papers' conclusions. Section IV.A focuses on articles that evaluate the performance of LWC algorithms. The researchers conducted hardware and software evaluations using various devices; for example, the hardware evaluation was performed using FPGA devices. The results show noticeable variation: some algorithms perform well on hardware, while others are better for software. The ten LWC algorithms can be applied to diverse practical environments. Interest in researching attacks on LWC algorithms has grown. Section IV.B addresses answers to RQ-3 and highlights key literature on cryptanalysis attacks. Despite extensive research, none of the existing security evaluations have broken the security claims of all algorithms.

Section IV.C addresses answers to RQ-4 and summarizes the article's contributions to improving and optimizing lightweight algorithms. Notwithstanding a lack of contributions in this field, their research advances efforts to improve the performance of LWC algorithms in hardware environments. This field is still in its early stages and requires extensive research to enhance algorithmic performance, moving beyond the current focus on a small subset of LWC methods. Utilizing optimization techniques for LWC algorithms, several studies [53], [55], [57] have reported encouraging results on resource-constrained devices, achieving up to a 30% performance improvement for the TinyJambu cipher through parallel LFSR implementation and a 38% reduction in computational overhead for ASCON. These results suggest further research, especially in the area of improving the effectiveness and usefulness of LWC optimization.

Section IV.D addressed RQ-5 by highlighting the key contributions of integrating LWC algorithms with systems and protocols. Although application-layer protocols were the only ones in the literature to use these LWC algorithms, they demonstrated encouraging latency and throughput efficiency, along with moderate resource consumption. This suggests the potential effectiveness of LWC algorithms in future applications and protocols. Finally, RQ-6 was addressed, leading to the identification of a fifth open research gap in Section V. Several gaps in the field of lightweight cryptography remain unaddressed, and future work aims to address some of these identified research gaps.

FUNDING

None.

ACKNOWLEDGEMENT

The author would like to thank the reviewers for their valuable contribution in the publication of this paper.

CONFLICTS OF INTEREST

The author declares no conflict of interest.

References

[1] S. Akhbarifar, H. H. S. Javadi, A. M. Rahmani and M. Hosseinzadeh, "RETRACTED ARTICLE: A secure remote health monitoring model for early disease diagnosis in cloud-based IoT environment," Personal and Ubiquitous Computing, vol. 27, no. 3, pp. 697-713, 2023.
[2] M. Lombardi, F. Pascale and D. Santaniello, "Internet of Things: A General Overview between Architectures, Protocols and Applications," Information, vol. 12, no. 2, 2021.
[3] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125-1142, 2017.
[4] J. H. Abawajy and M. M. Hassan, "Federated Internet of Things and Cloud Computing Pervasive Patient Health Monitoring System," Comm. Mag., vol. 55, no. 1, pp. 48-53, 1 2017.
[5] M. Maryska, P. Doucek, P. Sladek and L. Nedomova, "Economic Efficiency of the Internet of Things Solution in the Energy Industry: A Very High Voltage Frosting Case Study," Energies, vol. 12, no. 4, 2019.
[6] E. Bertino and N. Islam, "Botnets and Internet of Things Security," Computer, vol. 50, no. 2, pp. 76-79, 2017.
[7] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," IEEE Communications Surveys Tutorials, vol. 21, no. 3, pp. 2702-2733, 2019.
[8] A. Akbarzadeh, M. Bayat, B. Zahednejad, A. Payandeh and M. R. Aref, "A lightweight hierarchical authentication scheme for internet of things," Journal of Ambient Intelligence and Humanized Computing, vol. 10, no. 7, pp. 2607-2619, 2019.
[9] Y. Jiang, Y. Shen and Q. Zhu, "A Lightweight Key Agreement Protocol Based on Chinese Remainder Theorem and ECDH for Smart Homes," Sensors, vol. 20, no. 5, 2020.
[10] H. Qasim and M. Ibrahem, "Perfect Secrecy System Based on Chaotic Key Generator," Iraqi Journal of Information and Communication Technology, vol. 1, no. 2, pp. 1-12, 6 2018.
[11] K. Boeckl, M. Fagan, W. Fisher, N. Lefkovitz, K. N. Megas, E. Nadeau, D. G. O'Rourke, B. Piccarreta and K. Scarfone, "Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks," Gaithersburg, MD, 2019.
[12] M. Sonmez, K. McKay, C. Calik, Dong and L. Bassham, "Status Report on the First Round of the NIST Lightweight Cryptography Standardization Process," 4 2019.
[13] C. Dobraunig, M. Eichlseder, F. Mendel and M. Schläffer, "Ascon v1.2. Submission to NIST," NIST, 2021.
[14] G. M. Bertoni, J. Daemen and M. Peeters, "Keccak sponge function family main document," Submission to NIST (Round 2), vol. 3, 1 2009.
[15] S. Banik, A. Chakraborti, T. Iwata, K. Minematsu, M. Nandi, T. Peyrin, Y. Sasaki, S. M. Sim and Y. Todo, "GIFT-COFB: NIST LWC Second-round Candidate Status Update," Submitted to NIST Lightweight Cryptography,, 2020.

[16] M. Hell, T. Johansson, L. University, S. A. Maximov, E. Ab, W. Meier, J. Sönnerup and H. Yoshida, "Grain-128AEADv2-A lightweight AEAD stream cipher Cover sheet Corresponding submitter: Backup point of contact," NIST, Tokyo, 2020.

[17] C. Dobraunig, M. Eichlseder, S. Mangard, F. Mendel, B. Mennink, R. Primas and T. Unterluggauer, "ISAP v2.0. Submission to NIST," National Institute of Standards and Technology, 2021.

[18] A. Chakraborti, N. Datta, M. Nandi and K. Yasuda, "Beetle Family of Lightweight and Secure Authenticated Encryption Ciphers," IACR Transactions on Cryptographic Hardware and Embedded Systems, vol. 2018, no. 2, pp. 218-241, 5 2018.

[19] S. Kumar, J. Haj-Yahya, M. Khairallah, M. A. Elmohr and A. Chattopadhyay, "A Comprehensive Performance Analysis of Hardware Implementations of CAESAR Candidates," Cryptology ePrint Archive, 2017.

[20] C. Beierle, A. Biryukov, L. Cardoso dos Santos, J. Großschädl, A. Moradi, L. Perrin, A. Rezaei Shahmirzadi, A. Udovenko, V. Velichkov and Q. Wang, "Schwaemm and Esch: Lightweight Authenticated Encryption and Hashing using the Sparkle Permutation Family Corresponding submitter," National Institute of Standards and Technology (NIST), Paris, France, 2021.

[21] H. Wu and T. Huang, "JAMBU Lightweight Authenticated Encryption Mode and AES-JAMBU," NIST Lightweight Cryptography Workshop, 2015.

[22] G. Bertoni, J. Daemen, M. Peeters and G. Van Assche, "Duplexing the Sponge: Single-Pass Authenticated Encryption and Other Applications," Selected Areas in Cryptography, pp. 320-337, 2012.

[23] M. A. Jimale, M. R. Z'Aba, M. L. B. M. Kiah, M. Y. I. Idris, N. Jamil, M. S. Mohamad and M. S. Rohmad, "Authenticated Encryption Schemes: A Systematic Review," IEEE Access, vol. 10, pp. 14739-14766, 2022.

[24] R. S. Mahantesh and S. Mohapatra, "Design of Secured Block Ciphers PRESENT and HIGHT Algorithms and its FPGA Implementation," 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), pp. 1113-1118, 2018.

[25] Page MJ, McKenzie JE, Bossuyt PM, et al. Updating guidance for reporting systematic reviews: development of the PRISMA 2020 statement. J Clin Epidemiol. 2021;134:103-112.

[26] A. R. Alharbi, A. Aljaedi, A. Aljuhni, M. K. Alghuson, H. Aldawood and S. S. Jamal, "Evaluating Ascon Hardware on 7-Series FPGA Devices," IEEE Access, vol. 12, pp. 149076-149089, 2024.

[27] I. T. Abdel-Halim and H. M. Zayan, "Evaluating the Performance of Lightweight Block Ciphers for Resource-Constrained IoT Devices," 2022 4th Novel Intelligent and Leading Emerging Sciences Conference (NILES), pp. 39-44, 2022.

[28] I. Elsadek, S. Aftabjahani, D. Gardner, E. MacLean, J. R. Wallrabenstein and E. Y. Tawfik, "Hardware and Energy Efficiency Evaluation of NIST Lightweight Cryptography Standardization Finalists," 2022 IEEE International Symposium on Circuits and Systems (ISCAS), pp. 133-137, 2022.

[29] Y. Oh, K. Jang, A. Baksi and H. Seo, "Depth-Optimized Quantum Circuits for ASCON: AEAD and HASH," Mathematics, vol. 12, no. 9, 2024.

[30] Y. Watanabe, H. Yamamoto and H. Yoshida, "Performance Evaluation of NIST LWC Finalists on AVR ATmega and ARM Cortex-M3 Microcontrollers," Cryptology ePrint Archive, vol. 1, no. 1, pp. 1-8, 2022.

[31] M. Khairallah, T. Peyrin and A. Chattopadhyay, "Preliminary Hardware Benchmarking of a Group of Round 2 NIST Lightweight AEAD Candidates," Cryptology ePrint Archive, vol. 1, no. 1, pp. 1-163, 2020.

[32] C. Tezcan, "Analysis of Ascon, DryGASCON, and Shamash Permutations," International Journal of Information Security Science, vol. 9, no. 3, pp. 172-187, 2020.

[33] Q. Fu, Y. Luo, Q. Yang and L. Song, "Preimage and Collision Attacks on Reduced Ascon Using Algebraic Strategies," Cryptology ePrint Archive, vol. 1453, no. 1, pp. 1-39, 2023.

[34] Y. Chen, N. Zhang, X. Liang, L. Song, Q. Yang and Z. Feng, "Improving the Rectangle Attack on GIFT-64," Selected Areas in Cryptography – SAC 2023: 30th International Conference, Fredericton, Canada, August 14–18, 2023, Revised Selected Papers, pp. 43-61, 2024.

[35] M. Vaziri and V. Velichkov, "Conditional Cube Key Recovery Attack on Round-Reduced Xoodyak," Applied Cryptography and Network Security Workshops, vol. 13907, pp. 43-62, 10 2023.

[36] S. El Hirch, S. Mella, A. Mehrdad and J. Daemen, "Improved Differential and Linear Trail Bounds for ASCON," IACR Transactions on Symmetric Cryptology, vol. 2022, no. 4, pp. 145-178, 12 2022.

[37] O. Dunkelman, S. Ghosh and E. Lambooij, "Practical Related-Key Forgery Attacks on Full-Round TinyJAMBU-192/256," IACR Transactions on Symmetric Cryptology, vol. 2023, no. 2, pp. 176-188, 6 2023.

[38] S. Mella, J. Daemen and G. Van Assche, "Tighter Trail Bounds for Xoodoo," IACR Transactions on Symmetric Cryptology, vol. 2023, no. 4, pp. 187-214, 12 2023.

[39] L. Vialar, "Fast Side-Channel Key-Recovery Attack against Elephant Dumbo," NIST LWC Workshop, SSTIC, vol. 1, no. 1, pp. 1-13, 2022.

[40] M. Habu, K. Minematsu and T. Iwata, "Matching attacks on Romulus-M," IET Information Security, vol. 16, pp. 1-16, 1 2022.

[41] N. AmbiliK. and J. Jose, "Reinforcing Lightweight Authenticated Encryption Schemes against Statistical Ineffective Fault Attack," J. Cell. Autom., vol. 16, pp. 363-379, 2022.

[42] A. Inoue, T. Iwata and K. Minematsu, "Analyzing the Provable Security Bounds of GIFT-COFB and Photon-Beetle," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 13269 LNCS, pp. 67-84, 2022.

[43] M. Khairallah, "Security of COFB against Chosen Ciphertext Attacks," IACR Transactions on Symmetric Cryptology, vol. 2022, pp. 138-157, 1 2022.

[44] F. Liu, T. Isobe, W. Meier and Z. Yang, "Algebraic Attacks on Round-Reduced Keccak," Information Security and Privacy, vol. 13083, pp. 91-110, 2021.

[45] Y. Gao, Z. Zhang and Z. Zhang, "Differential Fault Attack of Lightweight Cipher GIFT Based on Byte Model," IEEE Internet of Things Journal, vol. 12, no. 1, pp. 435-444, 2025.

[46] R. Rohit, K. Hu, S. Sarkar and S. Sun, "Misuse-Free Key-Recovery and Distinguishing Attacks on 7-Round Ascon," IACR Transactions on Symmetric Cryptology, vol. 2021, no. 1, pp. 130-155, 3 2021.

[47] A. Kandi, A. Baksi, P. Gan, S. Guilley, T. Gerlich, J. Breier, A. Chattopadhyay, R. R. Shrivastwa, Z. Martinásek and S. Bhasin, "Side-Channel and Fault Resistant ASCON Implementation: A Detailed Hardware Evaluation," 2024 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), pp. 307-312, 2024.

[48] Y. Zhong and U. Guin, "Chosen-Plaintext Attack on Energy-Efficient Hardware Implementation of GIFT-COFB," 2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 73-76, 2022.

[49] H. Jiahui, "Stretching Cube Attacks: Improved Methods to Recover Massive Superpolies," Advances in Cryptology – ASIACRYPT 2022, pp. 537-566, 2022.
[50] D. Chang and M. S. Turan, "Recovering the Key from the Internal State of Grain-128AEAD," Cryptology ePrint Archive, vol. 1, no. 1, pp. 1-8, 1 2021.
[51] H. Zhou, R. Zong, X. Dong, K. Jia and W. Meier, "Interpolation Attacks on Round-Reduced Elephant, Kravatte and Xoofff," The Computer Journal, vol. 64, no. 4, pp. 628-638, 4 2021.
[52] R. Zong, X. Dong, H. Chen, Y. Luo, S. Wang and Z. Li, "Towards Key-recovery-attack Friendly Distinguishers: Application to GIFT-128," IACR Transactions on Symmetric Cryptology, vol. 2021, no. 1, pp. 156-184, 3 2021.
[53] I. Salam, T. H. Ooi, L. Xue, W.-C. Yau, J. Pieprzyk and R. C.-W. Phan, "Random Differential Fault Attacks on the Lightweight Authenticated Encryption Stream Cipher Grain-128AEAD," IEEE Access, vol. 9, pp. 72568-72586, 2021.
[54] L. Jellema and P. Schwabe, "Optimizing Ascon on RISC-V," Radboud University, 2019.
[55] M. El-Hadedy, R. Hua, K. Yoshii and W.-M. Hwu, "Optimizing ASCON Permutation in Multi-Clock Domains with Chisel: Resource Efficiency and Critical Path Reduction," 2024 IEEE 17th Dallas Circuits and Systems Conference (DCAS), pp. 1-6, 2024.
[56] C. Fernández-García, J. M. Mora-Gutiérrez and C. J. Jiménez-Fernández, "TinyJAMBU Hardware Implementation for Low Power," IEEE Access, vol. 12, pp. 108342-108349, 2024.
[57] A. D. R. Noor and M. O. Hasanuddin, "Using Esch256 Algorithm of the Sparkle Permutation Family to Enhance the Security of ESP-NOW Communication for Smart Lock Systems," 2024 10th International Conference on Wireless and Telematics (ICWT), vol. 1, no. 1, pp. 1-6, 2024.
[58] S. Windarta, S. Suryadi, K. Ramli, A. A. Lestari, W. Wildan, B. Pranggono and R. W. Wardhani, "Two New Lightweight Cryptographic Hash Functions Based on Saturnin and Beetle for the Internet of Things," IEEE Access, vol. 11, pp. 84074-84090, 2023.
[59] M. Naseer, S. Tariq and N. Riaz, "Substitution Layer Analysis of NIST Lightweight Cryptography Competition Finalists," 2022 19th International Bhurban Conference on Applied Sciences and Technology (IBCAST), pp. 659-664, 2022.
[60] Y.-C. Chen and W.-C. Ku, "A Security Improved IoT Authentication Protocol Based on Ascon Lightweight Cryptographic Algorithms," 2024 10th International Conference on Applied System Innovation (ICASI), pp. 229-231, 2024.
[61] V. Voloshyn, M. S. Khan, G. Srivastava and D. M, "Analysis of NIST Lightweight Cryptographic Algorithms Performance in IoT Security Environments based on MQTT," IEEE Wireless Communications and Networking Conference (WCNC), vol. 1, no. 1, pp. 1-6, 1 2024.
[62] C. Rahul, N. Kousarr, T. A. Yadav, P. Keerthi, S. Hariharan and V. Kukreja, "Unveiling time utilization in resource constrained environment," 2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS), vol. 1, pp. 1-6, 2024.
[63] W. BenMassaoud, D. M, R. H. Jhaveri and G. Srivastava, "Securing Internet of Vehicles Protocols using ASCON and GIFT-COFB," 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring), pp. 1-7, 2023.
[64] M. Nooruddin and D. Valles, "An Advanced IoT Framework for Long Range Connectivity and Secure Data Transmission Leveraging LoRa and ASCON Encryption," 2023 IEEE World AI IoT Congress (AIIoT), pp. 583-589, 2023.
[65] P. A. Wiradarma, A. T. Simamora, S. Lintang and M. O. Hasanuddin, "Enhancing Data Logger Telemetry Security for Go-Karts using GIFT-COFB Algorithm," 2023 International Conference on Electrical Engineering and Informatics (ICEEI), pp. 1-6, 2023.
[66] T. Al-Hasan, A. Sayed, F. Bensaali, A. Nhlabatsi and R. Hamila, "Security-Driven Performance Analysis of Lightweight Cryptography for Energy Efficiency Applications," 2024 IEEE 8th Energy Conference (ENERGYCON), vol. 1, no. 1, pp. 1-6, 1 2024.