Detailed review of lightweight PHOTON hash-based Signcryption approaches for IoT usage

Raghavendra A[1], Sai Kiran Oruganti[2]

[1] Postdoctoral Researcher, Lincoln University College, Malaysia;

[2] Professor, Lincoln University College, Malaysia;

Email ID: pdf.drRaghavendra@lincoln.edu.my, saisharma@lincoln.edu.my.

Abstract: As a result of the Internet of Things' (IoT) widespread use, a vast network of diverse, resource-constrained devices is constantly exchanging private information over dispersed networks. Because of the inadequate power, processing, and storage resources available, maintaining end-to-end secrecy, integrity, and authentication in these restricted circumstances continues to be an important issue. Despite being successful in lowering hardware complexity, current lightweight cryptographic techniques sometimes deal with hashing or encryption separately and lack a cohesive framework for signcryption. With an emphasis on PHOTON-based designs and signcryption techniques appropriate for IoT applications, this work methodically examines current developments in lightweight ciphers, hash functions, and authentication procedures published between 2021 and 2025. According to the investigation, PHOTON is still underrepresented in integrated signcryption contexts while demonstrating excellent diffusion and energy efficiency. A thorough assessment of FPGA platform performance reveals shortcomings in real-time validation, scalability, and key management. In order to overcome these constraints, the study encourages the development of a lightweight PHOTON hash-based signcryption architecture that balances security, power, area, and throughput trade-offs for IoT contexts with limited resources. The results help lay the groundwork for safe, scalable, and cost-effective IoT cryptographic systems, enabling real-world implementation in various fields.

Keywords: IoT; PHOTON hash; Signcryption; Lightweight Crptography; Hardware platform;

Introduction

Confidentiality and authentication are two essential communication security requirements. The validity and confidentiality of the message can usually be ensured using digital signatures and encryption. Either "encrypt before signing" or "sign before encryption" is the standard method for meeting both requirements at the same time. Nevertheless, there will be substantial intellectual and communication expenses associated with these. Signcryption not only meets these two security requirements at the same time, but it also has significantly lower computing and transmission expenses than the previously mentioned traditional methods [1]. The most effective way to communicate encrypted and verified data is through signcryption. As a result, it can also be used for mobile device authentication. The information that forms the basis of authentication usually consists of the following three categories of content: User biographical information, such as fingerprinting; User-owned goods, such as intelligent cards; and personally identifiable data, such as passwords. One-factor authentication is the common term used to

describe authentication using a password. The phrase "two-factor authentication" refers to smart card-based password authentication. Multifactor authentication uses two or more pieces of information to authenticate a user. There are several uses for encryption, such as online shopping, digital governance, and controlling keys.

Lightweight devices, such as Radio-Frequency Identification (RFID) cards and Internet of Things (IoT)-connected devices, are increasingly being used in daily activities for a number of purposes, such as monitoring and regulating or providing access to private data. These technological advances have created new challenges for cryptographers since they have the ability to leak and change confidential data utilizing low-processing devices, which can be costly. These devices should be safeguarded with a high level of authentication and have encryption techniques installed to avoid such circumstances. Conventional hash functions that demand a lot of processing power are inappropriate for such constrained systems. This resulted in the development of a number of lightweight authentication methods [2–3] and their use in the hardware and software of different platforms [4-6], as well as particular cryptanalysis procedures [7-8]. The internal architecture of the hash function approaches primarily focuses on the trade-offs between area and efficiency with different message digest length. Many of them have both effective software and hardware, while others may concentrate on either software or hardware. The current lightweight hashing methods require restricted processing power due to their utilization and resource constraints. However, these devices need to process data instantly. Thus, trade-offs between area and efficiency must be considered. PHOTON has small hardware and efficient software. Their permutation is similar to the LED block cipher, while having different data path and state size widths, even though they were first provided by the same collection [9–13].

Problem Statement: Numerous billions of gadgets with connectivity are constantly exchanging critical data over platforms with very few resources because of the IoT explosive growth. Because IoT nodes have limited processing power, energy storage, and memory capacities, maintaining confidentiality, integrity, and authentication in such systems continues to be a significant challenge. Even if they are secure, current cryptographic techniques frequently have significant overheads that make them inappropriate for lightweight applications. Recent research on hash functions and lightweight ciphers, such as PHOTON, Ascon, TinyJAMBU, and PRESENT, shows significant advancements in lowering power and area demands. Nevertheless, these methods are usually restricted to hashing or encryption by themselves, missing a combined structure that includes encryption and hash-based authentication (signcryption). Additionally, even if elliptic or hyperelliptic curve-based signcryption techniques offer robust security, their significant computation latency and energy costs make them inappropriate for real-time Internet of Things operations. Consequently, there is a research gap in creating a PHOTON hash-based signcryption technique that is lightweight, hardware-efficient, and scalable while achieving end-to-end data confidentiality, integrity, and authentication with the least amount of energy and hardware complexity. Secure key management, FPGA realizability, and performance scaling across various IoT contexts—ranging from sensor-level devices to edge and fog computing layers—must also be addressed by such a system.

Related Works

Lightweight cryptography has become crucial because traditional cryptographic algorithms have a substantial computational and power cost for protecting IoT gadgets with limited assets. Many scholars

have contributed to the optimization of hash and encryption designs for hardware efficiency. Al-Shatari et al. [14] enhanced PHOTON hash designs using iterative approaches, boosting speed by 51% and saving space by 60%, While Rashid et al. [15] developed an ECC-based accelerator with two-stage pipelining and Karatsuba multiplication, offering a 302× latency reduction. Windarta et al. [16] introduced ALIT-Hash and TJUILIK-Hash to accomplish sub-microsecond execution on integrated microcontrollers. Sideris et al. [18] and Santos Jr. et al. [20] revealed high-throughput FPGA-based versions of Keccak and SHA-256, with corresponding speeds of 38.043 Gbps and 1.4 Gbps. Similarly, AES and LED cipher variants have demonstrated energy-efficient encryption for small devices [25], [26]. Ali et al. [19] achieved considerable resistance against collision and brute-force attacks by implementing chaos-based hashing. These studies demonstrate how symmetric and optimum hashing methods can balance efficiency, area, and privacy for future IoT nodes.

Numerous studies have paired authenticated encryption methods with lightweight hash functions to ensure confidentiality and authenticity. Alharbi et al. [22], Khan et al. [23], and Tran et al. [24] demonstrated that Ascon, NIST's chosen AEAD standard, can reach throughput up to 8.8 Gbps with less area consumption. According to Fernández-García et al. [25] and Makhloufi et al. [26], TinyJAMBU and LED ciphers modified for IoT decreased power usage by 30–45%. While Ngo et al. [41] proposed a hybrid PRESENT/HMAC-PHOTON model that produced 182.9 Mbps throughput with minimal power consumption, Al-Shatari et al. [42] developed an LED–PHOTON AE approach with 46% less power and 14% area savings. Studies like Rajasekaran et al. [43] and Roy et al. [39], which achieved lower computational costs and communication delay, emphasized fog-assisted authentication. Malamas et al. [44] and Rullo et al. [46] also employed PUF-based authentication to increase device dependability and tamper resistance. Further hardware-focused developments looked on FPGA implementation and lightweight encryption technique optimization. Beaulieu et al. [28] and Bogdanov et al. [29] looked at SIMON and SPECK ciphers, which produce high throughput with little complicated hardware suitable for low-cost IoT applications. Banik et al. [30] introduced GIFT, which offers the best balance between area productivity and safety, while Bansod et al. [31] and Dey et al. [32] built PRESENT and RECTANGLE ciphers on FPGA, demonstrating lower gate count and power. Ravi et al. [34] and Sangeetha et al. [35] showed reduced latency and energy consumption with smaller substitution-permutation network (SPN) topologies, concentrating on the PRINCE and SKINNY ciphers. Majid et al. [36] created an area-efficient LEA cipher, while Praveen et al. [37] and Patil et al. [38] looked into better Ascon and Gimli topologies for IoT edge gadgets. When combined, these implementations show how lightweight block ciphers can be validated using an FPGA in terms of size, frequency, and energy efficiency criteria.

Recent advancements in hybrid and hash-assisted encryption techniques demonstrate the growing popularity of layered IoT protection. Singamaneni et al. [33] achieved 42% fewer kW and quicker key exchange than traditional ECC systems by employing ECC and PHOTON for hybrid encryption. Roy et al. [39] and Kumar et al. [40] developed mutual authentication architectures that lowered handshake duration by over 30% by using lightweight fundamentals for edge networks. Ngo et al. [41] and Al-Shatari et al. [42] verified the feasibility of integrating symmetric encryption and hashing to deliver authenticated encryption under limited power budgets. These linked architectures improve integrity and secrecy while reducing implementation difficulty.

Signcryption has lately emerged as a key element of Internet of Things security, combining encryption and digital signatures in a single process. Naresh et al. [47] introduced an identity-based online/offline

signcryption technique that shifts expensive calculations offline in order to lower real-time latency and power consumption. Kim et al. [48] enhanced LiSP (LiSP-XK) with lightweight ECC and Keccak-based hashing, increasing its efficiency for IIoT applications by 35%. Ali et al. [49] presented a hyperelliptic curve-based RFID signcryption technology that improved compute efficiency by 70% and transmission by 42%. Vidaković and Miliňvić [50] evaluated post-quantum signature techniques such as Dilithium, Falcon, and Sphincs+ and discovered trade-offs between resilience, performance, and storage. The premise that lightweight, hash-based signcryption offers a feasible path for scalable and energy-efficient IoT security frameworks is supported by all of this research, especially when using PHOTON and Ascon.

Method

The suggested technique employs a systematic review approach to examine recent advancements in signcryption, authentication, and lightweight cryptography that are relevant to IoT security. Figure 1 shows the methodology used for the literature review. The approach begins with an Introduction that describes the purpose and research backdrop, as well as the need for lightweight cryptographic solutions in IoT systems with restricted resources.

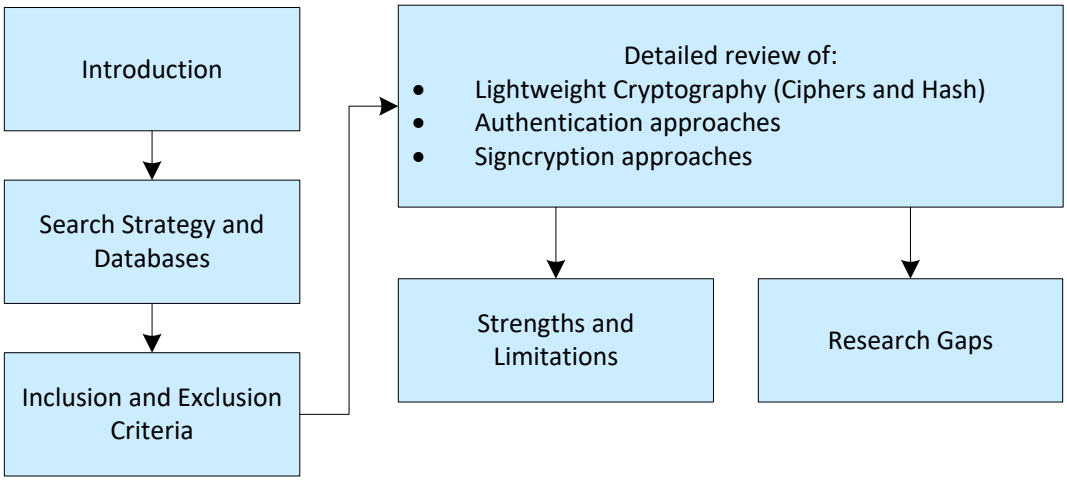

Figure 1. Methodology adopted for the literature review

Following that, a methodical search strategy was employed using a range of academic databases, such as IEEE Xplore, ScienceDirect, SpringerLink, and MDPI, to locate publications published between 2021 and 2025. Keywords such as "lightweight cryptography," "PHOTON hash," "IoT authentication," and "signcryption" were used to locate relevant material. Because of the inclusion and exclusion criteria (as described in Table 1), only peer-reviewed studies that directly addressed IoT security employing lightweight or hash-based encryption approaches were taken into investigation.

Following data gathering, the selected study was thoroughly evaluated and divided into three primary categories: (i) lightweight cryptography (including ciphers and hash functions), (ii) authentication methods, and (iii) signcryption approaches. Each area was analyzed with regard for algorithm design, implementation platform, and performance metrics. The results were then pooled to ascertain the benefits and drawbacks of earlier studies, establishing the framework for determining unfulfilled research needs.

This methodical methodology, in accordance with the PRISMA structure, ensures a comprehensive, impartial, and repeatable review process that leads to the development of specific research goals for developing a lightweight PHOTON hash-based signcryption system to support secure IoT applications.

Inclusion/Exclusion criteria

Table 1 lists the inclusion and exclusion criteria utilized in the literature selection procedure to ensure the caliber, applicability, and emphasis of the reviewed study. Publications published between 2021 and 2025 are given preference under the inclusion criteria, with an emphasis on research on PHOTON hash functions, lightweight cryptography, and signcryption methods meant for Internet of Things environments. Hardware-focused studies that have been released in peer-reviewed English-language journals or conferences with full-text access and comprehensive performance data, especially those implemented on FPGA or ASIC platforms, have been selected for investigation.

Table 1. Inclusion and Exclusion criteria of the proposed work

Criteria Type	Description	Inclusion Criteria	Exclusion Criteria
Publication Year	Time frame considered for the literature search	Studies published between 2021 and 2025	Studies published before 2020
Research Domain	Area of focus relevant to lightweight cryptography and IoT	Research related to PHOTON, hash-based, or lightweight cryptographic approaches for IoT	Studies unrelated to lightweight cryptography or IoT
Implementation Platform	Hardware or system used in implementation	Papers discussing hardware/FPGA/ASIC-based implementations	Works limited to software-only or simulation-based cryptography
Algorithm Focus	Cryptographic methods studied	Works focusing on hash-based encryption, signcryption, or PHOTON algorithms	Studies focusing on unrelated algorithms without lightweight relevance
Document Type	Type of publication	Peer-reviewed journal articles, conference papers, or open-access papers	Editorials, book chapters, or non-peer-reviewed content
Language	Language of publication	Papers written in English	Papers published in other languages
Data Availability	Access to full text and results	Papers with full-text access and detailed implementation metrics	Papers with restricted access or insufficient technical data
Relevance	Applicability to research goals	Directly related to signcryption and IoT hardware security	Not addressing encryption/signcryption or IoT security aspects

However, studies that focus on unrelated or non-lightweight cryptographic methods, software-only deployments, or studies published prior to 2020 are also disregarded. Additionally, non-peer-reviewed

content, restricted-access publications, and articles that did not address IoT security, encryption, or signcryption significance were excluded. This rigorous screening process ensures that only technically solid and context-specific studies that aligned with the objectives of lightweight PHOTON-based signcryption for IoT security were included in the systematic review.

Databases for conducting search

To guarantee accurate representation of both published and open-access investigations, the literature searching was carried out across four reputable and extensive academic databases:

- IEEE Xplore: Offers conference and journal articles most pertinent to lightweight cryptographic hardware, with a focus on electrical engineering, cryptography, FPGA, and IoT hardware implementations.
- Springer Link: Offers interdisciplinary research publications in embedded systems, computer science, and information security.
- ScienceDirect: Covers theoretical and applied research on hardware security implementations, IoT architecture, and lightweight cryptography.
- MDPI: Provides open-access research in hardware cryptography, electronics, and IoT security, making sure to incorporate the most recent developments in signcryption methods.

After adopting the inclusion and exclusion criteria, the initial pool of 3,867 publications from the search, which covered the years 2010–2025, was reduced to 50 final considered studies (2021–2025: Open Access). Table 2 lists the databases that were used in the execution of the work.

Table 2. Databases used in the work

Databases	2010-25	2021-25	OA	Final considered
IEEE Xplore	3,344	1,613	150	19
Springer Link	212	135	26	6
Science direct	173	143	49	7
MDPI	138	95	95	18
Total	3867	1986	320	50

Results and Discussion

Table 3 displays a performance summary of the lightweight cryptography methods currently in use on various FPGA platforms. The table compares several research designs, such as PHOTON, ASCON, TinyJAMBU, Keccak, SHA-3, and AES variations, based on critical hardware attributes, such as slice consumption, LUTs, flip-flops (FFs), clock cycles (CCs), maximum frequency, power usage, throughput, and efficiency. Of them, PHOTON-80/20/16 [14] has superior efficiency (4.33 Mbps/Slice) and a high throughput of 628 Mbps at 376 MHz, indicating that it has great promise for lightweight Internet of Things applications. In a similar vein, the ASCON family [21–24] provides modest throughput with variable trade-offs between resource use and power, while the TinyJAMBU and Ublock-TI designs demonstrate energy-efficient versions intended for constrained hardware.

By identifying significant variations in performance across FPGA generations (Artix-7, Virtex-7, Kintex-7, and Spartan-6), the results also demonstrate how architectural advancements and synthesis circumstances impact overall efficiency. High-throughput techniques like AES + Hamming Code and ASCON-128a offer outstanding efficiency, but they are less appropriate for ultra-low-power IoT nodes due to their higher hardware resource usage. However, algorithms like M-SPECK and Gimli Hash require less area at an additional cost of speed.

Table 3. Comparison of existing Hash and authentication approaches on the FPGA Platform

Designs	Approach	Data width	Slices	LUTs	FFs	CCs	Max. Fre (MHz)	Power (mW)	Throughput (Mbps)	Efficiency (Mbps/Slice)	FPGA
Ref [14]	PHOTON-80/20/16	100	145	363	188	60	376.43	82	628	4.33	Artix-7
Ref [15]	ECDH protocol	NA	5957	13105	2461	4942	316	NA	63.97	0.0107	Artix-7
Ref [18]	Keccak Hash	1152	1452	NA	NA	NA	396.28	NA	38.043	26.2	Viretx-7
Ref [20]	SHA-3	512	1933	6730		65	12.67	42	99.8	0.0516	Virtex-6
Ref [21]	ASCON-Sign 128s	32	NA	6500	5900	1027	150	270	4.67	NA	Artix-7
Ref [22]	ASCON-Sign 128a	64	303	1356	912	55	317	222	376	1.24	Artix-7
Ref [24]	ASCON-128a	128	2812	6536	NA	NA	98.2	104	8806	3.14	Viretx-7
REF [25]	TinyJAMBU	32	172	381	294	NA	NA	86.89	NA	NA	Artix-7
Ref [26]	AES + Hamming Code	128	1650`	3145	NA	NA	224.26	NA	2870.48	1.739	Virtex-4
Ref [30]	M-SPECK	32	NA	240	0	NA	153.85	175	NA	NA	Artix-7
Ref [31]	Ublock-TI	32	289	773	707		324.94	NA	NA	NA	Kintex-7
REF [32]	Blowfish	64	4576	5778	6325	4.9	100	210	1292	0.2823	Artix-7
REF [37]	Gimli Hash	NA	873	1036	NA	74	429.8	1.04	740	0.84	Spartan-6
REF [37]	Gimli -AE	NA	1291	1715	NA	122	408.59	15.4	420	0.33	Spartan-6
REF [39]	APUF–DIES-IoT	NA	9	21	36	NA	742.45	NA	NA	NA	Virtex-6
Ref [40]	ChaCha20–Poly1305 AE	NA	NA	10808	3731	NA	166	NA	948	NA	Viretx-7
REF [42]	LED+PHOTON	NA	1030	NA	NA	140	140.39	99.3	NA	NA	Cyclone-II
Ref [45]	Ascon-XOF128	NA	4285	3490	NA	NA	100	NA	NA	NA	Artix-7

The comparative study highlights a major research requirement, which is the absence of one architecture that achieves balanced trade-offs among area, power, throughput, and security. The PHOTON-based approaches ([14], [42]) exhibit promising results due to their compact structure and resilient diffusion properties, even though they have not yet been fully developed into integrated signcryption frameworks. A lightweight PHOTON hash-based signcryption method that can offer superior security and efficiency on an FPGA for useful IoT applications is therefore required.

Strengths and Limitations

Strengths: The literature review demonstrates remarkable progress in the development of lightweight cryptographic primitives designed for Internet of Things environments. Algorithms like PHOTON [14] and PLWHF [35] have shown remarkable hardware effectiveness when compared to conventional ciphers, with up to 60% area and 40% power reductions. High-performance variations like as Keccak [18], Ascon [22], and Ascon-128a [24] have exhibited multi-Mbps throughput, indicating their real-time potential for

restricted IoT devices. Furthermore, several studies have proposed hybrid cryptographic frameworks as ECC + PHOTON [33] and LED–PHOTON [42] that effectively integrate encryption and authentication with low overhead. Additionally, by increasing device-level trust and providing rapid identity verification, fog-assisted and PUF-based systems [39], [44], and [46] enhanced system durability against unauthorized access. Because solutions like Ascon [23] and Gimli [37] are scalable, both efficiency and safety may be balanced by different criteria across IoT tiers. Notably, identity-based and elliptic curve-based signcryption approaches [47-49] significantly decreased computation costs while preserving data secrecy and authenticity, and novel post-quantum cryptography algorithms [50] showed forward-compatible robustness to later connected devices.

Limitations: Despite these advancements, a number of important problems remain unresolved. Most of the suggested techniques have only been evaluated by simulation or FPGA-level tests and lack comprehensive real-world IoT deployment evaluations [14], [28], and [47]. The incorporation of AEAD, hash, and signcryption units introduces design complexity that leads to increased verification costs and temporal closure problems in FPGA synthesis [41], [42]. Efforts to reduce power consumption frequently outcome in an energy-security trade-off since reduced utilizing resources may weaken susceptibility to side-channel or quantum attacks [36], [48]. Additionally, lightweight approaches typically exhibit poor scalability across disparate IoT devices with different resource capacities [25], [43]. The absence of robust key management strategies, such as private key generation, revocation, and synchronization, further restricts their usage in distributed systems [15], [47]. Finally, many existing approaches are application-specific, focusing just on RFID, IIoT, or cloud computing environments, which restricts their generalizability and cross-domain usage [39], [49].

Research Gaps

Based on the findings of the review mentioned above, a few research gaps have been identified and are stated as follows:

- ***Absence of a Unified Framework:*** The majority of current research concentrates on lightweight hashing or encryption independently; very few combine signcryption and PHOTON-based hashing in a unified framework appropriate for Internet of Things applications [14], [41], and [42].
- ***Minimal Lightweight Signcryption Implementations:*** The majority of current signcryption algorithms [47]–[49] rely on elliptic or hyperelliptic curve encryption, which is still computationally costly and inappropriate for extremely constrained Internet of Things nodes.
- ***Lack of Optimized PHOTON-Based Signcryption:*** Although PHOTON has been effectively employed for hashing and authentication [14], [41], and [42], its possible incorporation into a complete signcryption method for confidentiality and authentication has not been investigated.
- ***Hardware-Performance Trade-Off Ignored:*** While many studies emphasize power or area gains, few offer balanced optimization across latency, throughput, power, and area under a single lightweight architecture. [16], [18], [23], [25].

- ***Absence of FPGA and Real-Time IoT Assessment:*** A number of research [19], [29], and [34] validate strategies solely using simulation or software tools, lacking FPGA-based or real-time IoT deployment to evaluate efficiency under realistic communication loads.
- ***Improper Key Management and Scalability:*** Secure key generation, distribution, and lifecycle management across diverse IoT layers (sensor–edge–fog–cloud) are rarely addressed by lightweight encryption and authentication techniques. [39], [43].
- ***Limited Benchmarking Across Platforms:*** It is challenging to assess genuine lightweight performance since FPGA, ASIC, and microcontroller implementations lack standard comparisons measures (such as energy efficiency and throughput/area ratio) [23], [25], and [31].
- ***Ignored Hash–Authentication Co-Design:*** Although hash-based integrity is crucial in the Internet of Things, the optimization of hashing (PHOTON) in conjunction with encryption and authentication is still not well studied [35], [37], and [38].
- ***Requirement for Application-Level Validation:*** There aren't many studies that connect cryptographic hardware outcomes to particular Internet of Things use cases (such fog-assisted networks, smart locks, or sensor authentication), which reduces application relevance [42], [47], and [49].

Conclusion

This work provided a methodical evaluation of current lightweight cryptography algorithms with a focus on PHOTON-based hash functions, authentication schemes, and signcryption techniques relevant to IoT security. Although various algorithms, such ASCON, Keccak, and TinyJAMBU, have shown significant hardware efficiency and throughput, the analysis found that these algorithms frequently lack integrated confidentiality–authentication mechanisms and strong key management appropriate for heterogeneous IoT networks. Additionally, a lot of FPGA-based systems are still restricted to prototype evaluation, with little research done on real-world implementation or resistance to side-channel and quantum hazards. This study highlights the necessity for a lightweight PHOTON hash-based signcryption paradigm that can provide complete security amenities—encryption, authentication, and integrity—in a single, hardware-optimized design in order to overcome these constraints. The suggested framework seeks to retain minimal implementation costs while balancing power, area, and performance to provide adaptation across IoT tiers. Future research will concentrate on creating and verifying this architecture on FPGA platforms, assessing its effectiveness in a variety of IoT applications, and strengthening its resistance to new post-quantum and physical-layer threats.

References

1. C. Silva, V. A. Cunha, J. P. Barraca, and R. L. Aguiar, “Analysis of the cryptographic algorithms in IoT communications,” *Inf. Syst. Front.*, vol. 26, no. 4, pp. 1243–1260, 2024, doi: 10.1007/s10796-023-10383-9.
2. M. A. Caraveo-Cacep, R. Vázquez-Medina, and A. Hernández Zavala, “A survey on low-cost development boards for applying cryptography in IoT systems,” *Internet Things (Amst.)*, vol. 22, no. 100743, p. 100743, 2023, doi: 10.1016/j.iot.2023.100743.
3. S. Kumar, D. Kumar, R. Dangi, G. Choudhary, N. Dragoni, and I. You, “A review of lightweight security and privacy for resource-constrained IoT devices,” *Comput. Mater. Contin.*, vol. 78, no. 1, pp. 31–63, 2024, doi: 10.32604/cmc.2023.047084.

4. M. El-hajj, H. Mousawi, and A. Fadlallah, “Analysis of lightweight cryptographic algorithms on IoT hardware platform,” *Future Internet*, vol. 15, no. 2, p. 54, 2023, doi: 10.3390/fi15020054.
5. A. Hkiri, M. Karmani, F. H. Alasmary, O. Ben Bahri, A. M. Murayr, and M. Machhout, “In-depth study of lightweight block ciphers: Performance assessment and implementation on sensor motes,” *Alex. Eng. J.*, vol. 113, pp. 461–479, 2025, doi: 10.1016/j.aej.2024.11.023.
6. K. U. Sarker, “A systematic review on lightweight security algorithms for a sustainable IoT infrastructure,” *Discov. Internet Things*, vol. 5, no. 1, 2025, doi: 10.1007/s43926-025-00150-4.
7. D. A. N. Gookyi and K. Ryoo, “A lightweight System-on-Chip based cryptographic core for low-cost devices,” *Sensors (Basel)*, vol. 22, no. 8, p. 3004, 2022, doi: 10.3390/s22083004.
8. I. Cetintav and M. Tahir Sandikkaya, "A Review of Lightweight IoT Authentication Protocols From the Perspective of Security Requirements, Computation, Communication, and Hardware Costs," in *IEEE Access*, vol. 13, pp. 37703-37723, 2025, doi: 10.1109/ACCESS.2025.3546147.
9. M. Abdalzaher, M. Fouda, A. Emran, Z. Fadlullah, and M. Ibrahem, “A survey on key management and authentication approaches in smart metering systems,” *Energies*, vol. 16, no. 5, p. 2355, 2023, doi: 10.3390/en16052355.
10. R. Chen and B. Li, “Exploration of the high-efficiency hardware architecture of SM4-CCM for IoT applications,” *Electronics (Basel)*, vol. 11, no. 6, p. 935, 2022, doi: 10.3390/electronics11060935.
11. X. Zhang *et al.*, “Design and analysis of area and energy efficient reconfigurable cryptographic accelerator for securing IoT Devices,” *Sensors (Basel)*, vol. 22, no. 23, p. 9160, 2022, doi: 10.3390/s22239160.
12. M. M. Hazzazi, S. Attuluri, Z. Bassfar, and K. Joshi, “A novel cipher-based data encryption with Galois field theory,” *Sensors (Basel)*, vol. 23, no. 6, p. 3287, 2023, doi: 10.3390/s23063287.
13. Y. Salomo, I. Syafalni, N. Sutisna and T. Adiono, "Hardware-Software Stitching Algorithm in Lightweight Q-Learning System on Chip (SoC) for Shortest Path Optimization," in *IEEE Access*, vol. 13, pp. 105044-105062, 2025, doi: 10.1109/ACCESS.2025.3578681.
14. M. O. A. Al-Shatari, F. A. Hussin, A. A. Aziz, G. Witjaksono and X. -T. Tran, "FPGA-Based Lightweight Hardware Architecture of the PHOTON Hash Function for IoT Edge Devices," in *IEEE Access*, vol. 8, pp. 207610-207618, 2020, doi: 10.1109/ACCESS.2020.3038219.
15. M. Rashid, H. Kumar, S. Z. Khan, I. Bahkali, A. Alhomoud, and Z. Mehmood, “Throughput/area optimized architecture for elliptic-curve Diffie-Hellman protocol,” *Appl. Sci. (Basel)*, vol. 12, no. 8, p. 4091, 2022, doi: 10.3390/app12084091.
16. S. Windarta *et al*., "Two New Lightweight Cryptographic Hash Functions Based on Saturnin and Beetle for the Internet of Things," in *IEEE Access*, vol. 11, pp. 84074-84090, 2023, doi: 10.1109/ACCESS.2023.3301128.
17. S.-T. Wu, “A key-based multi-mode clock-controlled stream cipher for real-time secure communications of IoT,” *Electronics (Basel)*, vol. 12, no. 5, p. 1076, 2023, doi: 10.3390/electronics12051076.
18. A. Sideris, T. Sanida, and M. Dasygenis, “A novel hardware architecture for enhancing the Keccak hash function in FPGA devices,” *Information (Basel)*, vol. 14, no. 9, p. 475, 2023, doi: 10.3390/info14090475.

19. A. A. M. A. Ali, M. J. Hazar, M. Mabrouk, and M. Zrigui, “Proposal of a modified hash algorithm to increase blockchain security,” *Procedia Comput. Sci.*, vol. 225, pp. 3265–3275, 2023, doi: 10.1016/j.procs.2023.10.320.
20. A. E. B. Santos Jr, L. M. D. da Silva, M. F. Torquato, S. N. Silva, and M. A. C. Fernandes, “SHA-256 hardware proposal for IoT devices in the blockchain context,” *Sensors (Basel)*, vol. 24, no. 12, p. 3908, 2024, doi: 10.3390/s24123908.
21. Magyari and Y. Chen, “Securing the internet of things with ascon-sign,” *Internet Things (Amst.)*, vol. 28, no. 101394, p. 101394, 2024, doi: 10.1016/j.iot.2024.101394.
22. A. R. Alharbi, A. Aljaedi, A. Aljuhni, M. K. Alghuson, H. Aldawood and S. S. Jamal, "Evaluating Ascon Hardware on 7-Series FPGA Devices," in *IEEE Access*, vol. 12, pp. 149076-149089, 2024, doi: 10.1109/ACCESS.2024.3471694.
23. S. Khan *et al.*, “Securing the IoT ecosystem: ASIC-based hardware realization of Ascon lightweight cipher,” *Int. J. Inf. Secur.*, vol. 23, no. 6, pp. 3653–3664, 2024, doi: 10.1007/s10207-024-00904-1.
24. S. -N. Tran, V. -T. Hoang and D. -H. Bui, "A Hardware Architecture of NIST Lightweight Cryptography Applied in IPSec to Secure High-Throughput Low-Latency IoT Networks," in *IEEE Access*, vol. 11, pp. 89240-89248, 2023, doi: 10.1109/ACCESS.2023.3306420.
25. A. Fernández-García, J. M. Mora-Gutiérrez and C. J. Jiménez-Fernández, "TinyJAMBU Hardware Implementation for Low Power," in *IEEE Access*, vol. 12, pp. 108342-108349, 2024, doi: 10.1109/ACCESS.2024.3438378.
26. A. EL Makhloufi, S. EL Adib, and N. Raissouni, “Hardware pipelined architecture with reconfigurable key based on the AES algorithm and hamming code for the earth observation satellite application: Sentinel-2 satellite data case,” *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 8, no. 100548, p. 100548, 2024, doi: 10.1016/j.prime.2024.100548.
27. S. Ahmed *et al*., "Lightweight AES Design for IoT Applications: Optimizations in FPGA and ASIC With DFA Countermeasure Strategies," in *IEEE Access*, vol. 13, pp. 22489-22509, 2025, doi: 10.1109/ACCESS.2025.3533611.
28. M. Imdad, A. Fazil, S. N. B. Ramli, J. Ryu, H. B. Mahdin, and Z. Manzoor, “DNA-PRESENT: An improved security and low-latency, lightweight cryptographic solution for IoT,” *Sensors (Basel)*, vol. 24, no. 24, p. 7900, 2024, doi: 10.3390/s24247900.
29. G. Cagua, V. Gauthier-Umaña and C. Lozano-Garzon, "Implementation and Performance of Lightweight Authentication Encryption ASCON on IoT Devices," in *IEEE Access*, vol. 13, pp. 16671-16682, 2025, doi: 10.1109/ACCESS.2025.3529757.
30. R. Mohanapriya and V. Nithish Kumar, "Modified SPECK (M-SPECK) Lightweight Cipher Architecture for Resource-Constrained Applications," in *IEEE Access*, vol. 13, pp. 88993-89002, 2025, doi: 10.1109/ACCESS.2025.3570727.
31. B. Liu and M. Tang, "A Very Compact and a Threshold Implementation of uBlock for Internet of Things," in *Tsinghua Science and Technology*, vol. 30, no. 5, pp. 2270-2283, October 2025, doi: 10.26599/TST.2024.9010257.
32. J. A. Prathap and M. Sathiyanarayanan, "Fault Detection in Blowfish Algorithm Using FPGA-Based Modified Decision Tree Approach," in *IEEE Access*, vol. 13, pp. 90591-90600, 2025, doi: 10.1109/ACCESS.2025.3567659.

33. K. K. Singamaneni, “A novel lightweight hybrid cryptographic framework for secure smart card operations,” *EURASIP J. Inf. Secur.*, vol. 2025, no. 1, 2025, doi: 10.1186/s13635-025-00204-8.
34. B. W. Aboshosha, M. M. Zayed, H. S. Khalifa, and R. A. Ramadan, “Enhancing Internet of Things security in healthcare using a blockchain-driven lightweight hashing system,” *Beni-Suef Univ. J. Basic Appl. Sci.*, vol. 14, no. 1, 2025, doi: 10.1186/s43088-025-00644-8.
35. A. Sevin, “Implementation of a data-parallel approach on a lightweight hash function for IoT devices,” *Mathematics*, vol. 13, no. 5, p. 734, 2025, doi: 10.3390/math13050734.
36. A. Aslan, “Energy consumption analysis of ISO/IEC 29192-2 standard lightweight ciphers,” *Appl. Sci. (Basel)*, vol. 15, no. 7, p. 3928, 2025, doi: 10.3390/app15073928.
37. S. Khan, W. -K. Lee and S. O. Hwang, "A Flexible Gimli Hardware Implementation in FPGA and Its Application to RFID Authentication Protocols," in *IEEE Access*, vol. 9, pp. 105327-105340, 2021, doi: 10.1109/ACCESS.2021.3100104.
38. M. N. Sudha, M. Rajendiran, M. Specht, K. S. Reddy, and S. Sugumaran, “A low-area design of two-factor authentication using DIES and SBI for IoT security,” *J. Supercomput.*, vol. 78, no. 3, pp. 4503–4525, 2022, doi: 10.1007/s11227-021-04022-w.
39. K. S. Roy, S. Deb, and H. K. Kalita, “A novel hybrid authentication protocol utilizing lattice-based cryptography for IoT devices in fog networks,” *Digit. Commun. Netw.*, vol. 10, no. 4, pp. 989–1000, 2024, doi: 10.1016/j.dcan.2022.12.003.
40. R. Serrano, C. Duran, M. Sarmiento, C.-K. Pham, and T.-T. Hoang, “ChaCha20–Poly1305 Authenticated Encryption with additional data for transport Layer Security 1.3,” *Cryptography*, vol. 6, no. 2, p. 30, 2022, doi: 10.3390/cryptography6020030.
41. C. T. Ngo, J. K. Eshraghian, and J.-P. Hong, “An area-optimized and power-efficient CBC-PRESENT and HMAC-PHOTON,” *Electronics (Basel)*, vol. 11, no. 15, p. 2380, 2022, doi: 10.3390/electronics11152380.
42. M. Al-Shatari, F. A. Hussin, A. A. Aziz, T. A. E. Eisa, X.-T. Tran, and M. E. E. Dalam, “IoT edge device security: An efficient lightweight authenticated encryption scheme based on LED and PHOTON,” *Appl. Sci. (Basel)*, vol. 13, no. 18, p. 10345, 2023, doi: 10.3390/app131810345.
43. S. Rajasekaran, A. Maria, B. P. Chapa and A. R. Gondu, "FAV2G: Fog-Based Authentication Scheme for Vehicle-to-Grid Network With Verilog Implementation," in *IEEE Open Journal of the Computer Society*, vol. 6, pp. 1512-1524, 2025, doi: 10.1109/OJCS.2025.3613959.
44. V. Malamas, P. Kotzanikolaou, K. Nomikos, C. Zonios, V. Tenentes and M. Psarakis, "HA-CAAP: Hardware-Assisted Continuous Authentication and Attestation Protocol for IoT Based on Blockchain," in *IEEE Internet of Things Journal*, vol. 12, no. 11, pp. 15650-15666, 1 June1, 2025, doi: 10.1109/JIOT.2025.3530775.
45. M. Gladis Kurian and Y. Chen, “Ascon on FPGA: Post-quantum safe Authenticated Encryption with replay protection for IoT,” *Electronics (Basel)*, vol. 14, no. 13, p. 2668, 2025, doi: 10.3390/electronics14132668.
46. Rullo *et al*., "PUF-Based Authentication-Oriented Architecture for Identification Tags," in *IEEE Transactions on Dependable and Secure Computing*, vol. 22, no. 1, pp. 66-83, Jan.-Feb. 2025, doi: 10.1109/TDSC.2024.3387568.

47. V. S. Naresh, S. Reddi, S. Kumari, V. V. L. D. Allavarpu, S. Kumar and M. -H. Yang, "Practical Identity Based Online/Off-Line Signcryption Scheme for Secure Communication in Internet of Things," in *IEEE Access*, vol. 9, pp. 21267-21278, 2021, doi: 10.1109/ACCESS.2021.3055148.
48. T. -H. Kim, G. Kumar, R. Saha, W. J. Buchanan, T. Devgun and R. Thomas, "LiSP-XK: Extended Light-Weight Signcryption for IoT in Resource-Constrained Environments," in *IEEE Access*, vol. 9, pp. 100972-100980, 2021, doi: 10.1109/ACCESS.2021.3097267.
49. U. Ali *et al*., "RFID Authentication Scheme Based on Hyperelliptic Curve Signcryption," in *IEEE Access*, vol. 9, pp. 49942-49959, 2021, doi: 10.1109/ACCESS.2021.3069429.
50. M. Vidaković and K. Miličević, “Performance and applicability of post-quantum digital signature algorithms in resource-constrained environments,” *Algorithms*, vol. 16, no. 11, p. 518, 2023, doi: 10.3390/a16110518.