AI Detector *by SciSpace*

Comparative_Analysis_of_Lightweight_Cryptographic_Algorithms_Across_Key_IoT_Domains__Healthcare__Agriculture__Industrial_IoT__a.pdf • 26 November 2025
2820 words (21142 characters)

Mostly AI **72%**

The text is almost entirely produced using AI, with tiny to no human contribution.

AI weightage	Content weightage	Sentences
H Highly AI written	**19%** Content	27
M Moderately AI written	**16%** Content	22
L Lowly AI written	**7%** Content	10

A Domain-Specific Comparative Review of Lightweight Cryptographic Algorithms for IoT Systems

Anshul Chaudhary[1], Manesh Sharma[2], and Dr. Nirmalya Kar[3]
Department of Computer Science and Engineering, National Institute of Technology, Agartala, India
[1]*anshulcruck@gmail.com*, [2]*gautamanesh2469@gmail.com*, [3]*nirmalya@ieee.org*

***Abstract*—Lightweight cryptography has become essential for securing modern Internet of Things (IoT) systems, where devices operate with limited memory, computation, and power resources. This paper presents a domain-based comparison of widely used lightweight ciphers, focusing on their suitability for constrained environments such as healthcare, agriculture, smart cities, and Industrial IoT (IIoT). The analysis considers hardware cost, energy usage, latency, throughput, internal structure, and key size for ciphers including PRESENT, SIMON, LED, KTANTAN, RECTANGLE, PRINCE, Piccolo, ASCON and QARMA. Results show that algorithms such as PRESENT and SIMON provide high energy efficiency for long-term sensing in agriculture and medical monitoring, while high-speed ciphers like PRINCE and RECTANGLE are more appropriate for real-time automation in smart cities and industrial systems. This study highlights that the optimal choice of lightweight cryptography depends on the specific requirements of each IoT domain, rather than a single performance metric.**

***Index Terms*—Lightweight Cryptography, Internet of Things (IoT), Block Ciphers, Authenticated Encryption, Resource-Constrained Devices, Smart Healthcare, Smart Agriculture, Smart Cities, Industrial IoT.**

I. Introduction

A. *Overview of IoT and Its Security Challenges*

The Internet of Things (IoT) connects large numbers of sensors, processors, and embedded devices that exchange data for automation and decision making. These systems are now widely used in healthcare monitoring, smart agriculture, industrial control, transportation, and public infrastructure. Since many IoT devices handle sensitive information and operate in unattended environments, secure communication is required to prevent data leakage, manipulation, or unauthorized access. However, most IoT nodes are built with limited memory, small batteries, and low-power processors, which makes it difficult to implement conventional cryptographic techniques without affecting system performance or device lifetime.

Traditional algorithms such as RSA and AES were originally designed for high-performance computing platforms. Their high computational and memory demands lead to significant energy consumption when applied to small embedded nodes. In many cases, using these algorithms results in slow execution, frequent battery drain, and increased communication delay, which is unsuitable for real-time and long-term IoT deployments. These limitations highlight the need for security methods that offer strong protection while maintaining low resource usage.

Lightweight cryptography addresses the limitations of traditional algorithms by providing secure encryption and authentication with minimal computational overhead. LWC techniques are specifically optimized for low-power, low-cost, and memory-restricted platforms. These algorithms aim to provide confidentiality, integrity, and authentication without reducing device performance. As a result, lightweight cryptography is now considered a practical and necessary security solution for many IoT applications that must operate continuously with limited resources.

B. *Motivation and Scope of This Study*

Although several lightweight algorithms have been proposed, selecting an appropriate cipher for a specific IoT domain remains challenging. Existing research commonly evaluates algorithms based on theoretical metrics such as area cost or latency, but does not provide clear guidelines for choosing suitable ciphers for different real-world applications. This paper aims to address this gap by presenting a domain-specific comparison of popular lightweight ciphers. The study evaluates PRESENT, SIMON, LED, KTANTAN, RECTANGLE, PRINCE, Piccolo, ASCON and QARMA with respect to their suitability for healthcare devices, agricultural sensing systems, smart city infrastructure, and Industrial IoT environments. The objective is to help researchers and developers identify ciphers that provide the best balance between security, performance, and energy efficiency for their intended IoT domain.

II. Review of Earlier Work

PRESENT: PRESENT is one of the earliest lightweight block ciphers, introduced in 2007 by Bogdanov et al. using a compact Substitution–Permutation Network (SPN) structure [1]. It encrypts 64-bit data with key options of 80 and 128 bits

over 31 rounds, employing sixteen 4-bit S-boxes followed by a bitwise permutation [1]. Due to its very small gate count and low power requirements, PRESENT is highly suitable for long-term field deployments such as agricultural monitoring nodes and wearable medical sensors.

SIMON: Proposed by Beaulieu et al. in 2013, the SIMON family supports multiple word and key sizes, denoted SIMON2n/mn, with a Feistel-based structure designed for energy-efficient hardware implementation [6]. For example, SIMON64/128 operates on a 64-bit block using a 128-bit key. While its throughput remains lower than other candidates, SIMON offers excellent energy efficiency, making it advantageous for passive IoT nodes that rely on small batteries or intermittent power sources.

LED: The LED cipher integrates concepts from PRESENT, compact AES implementations [4], and PHOTON [5], and uniquely performs encryption without a key schedule [3]. It supports 64–128 bit keys and requires only 966–1265 GE, depending on security level [7]. The absence of a key expansion mechanism reduces area cost, making LED well-suited for compact biomedical devices, although it increases susceptibility to related-key attacks [6].

RECTANGLE: RECTANGLE adopts a bit-sliced lightweight SPN architecture and completes encryption in only 25 rounds—fewer than PRESENT's 31 [8]. Its efficient bit-wise operations yield higher throughput on constrained hardware, which is beneficial in latency-sensitive networks such as traffic automation, smart lighting, and other real-time smart-city infrastructures.

PRINCE: PRINCE targets low-latency encryption and decrypts data using a 64-bit block and 128-bit key through only 12 rounds [9], [10]. With low energy usage (5.53 J/bit) and minimal delay, it achieves 533.3 Kb/s throughput while occupying 2953 GE [11]. This deterministic low latency makes PRINCE ideal for time-critical control systems in smart grids and IIoT automation.

Piccolo: Piccolo supports 80-bit and 128-bit keys and performs 25 or 31 rounds on a 64-bit block, requiring as little as 432 GE for its smallest configuration [12]. Its compactness makes it highly suitable for ultra-constrained IoT devices such as RFID tags used in logistics, retail, and smart-asset tracking systems.

KTANTAN: Designed for extremely small IoT hardware, KTANTAN and its variant KATAN operate using an 80-bit key and block sizes of 32–64 bits, requiring only 462–802 GE [13]. Although its non-modifiable key limits flexibility, its compact footprint enables cost-efficient authentication in RFID-based IIoT systems. However, reduced-round versions are vulnerable to meet-in-the-middle cryptanalysis [15], and software execution suffers from high bit manipulation overhead [14].

ASCON: ASCON is a single-pass nonce-based authenticated encryption scheme that offers strong resistance against side-channel attacks and supports resource-efficient implementation on embedded systems [16], [17]. Recognized as the CAESAR competition winner in 2023 and standardized as ISO/IEC 29192-5:2019, ASCON is a promising choice for secure medical data transmission and smart-grid communication networks.

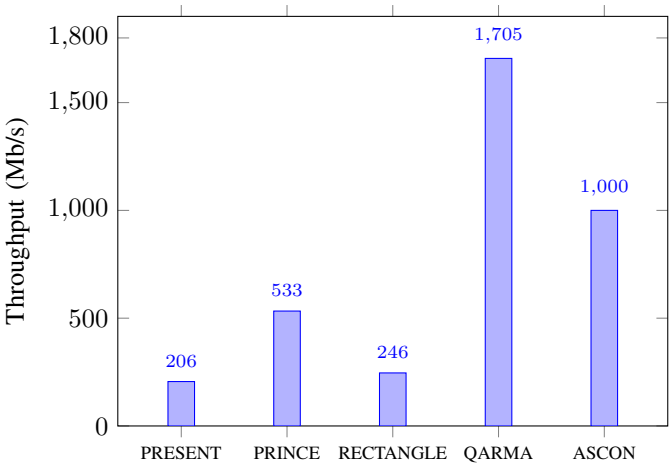

Fig. 1. Throughput comparison of selected lightweight ciphers.

QARMA: QARMA is a tweakable block cipher inspired by reflective structures such as PRINCE and MANTIS, built using a three-round Even-Mansour construction [18], [19]. With equal block and tweak sizes of 64 or 128 bits, QARMA is highly suited for secure memory encryption in automotive and industrial processors including Armv8-A systems [20]. Its reduced-round versions, however, exhibit vulnerabilities to MITM-based attacks [21].

SAT_Jo: SAT_Jo is an SPN-based lightweight cipher for IoT tags, utilizing a 4×4 S-box over $\mathbb{F}_{2^4}$ and running 31 rounds with an 80-bit key [23]. While effective in constrained RFID environments, its similarity to PRESENT exposes it to integral distinguishers [23]. Furthermore, the lack of support on platforms such as Arduino and Raspberry Pi limits its practical deployment despite favorable hardware efficiency [24].

TABLE I
COMPARISON OF SELECTED LIGHTWEIGHT CRYPTOGRAPHIC ALGORITHMS

Algorithm (name)	Key (bits)	Block (bits)	Rounds (count)	GE (units)	Latency (cycles)	Throughput (Mb/s)
PRESENT	80/128	64	31	2195	31	206
SIMON	64/72/96/128	32/48/64	32/52/72	763	304	15.8
LED	64/80/96/128	64	32/48	966–1265	–	133.3
RECTANGLE	128	64	25	1787	26	246
PRINCE	128	64	12	2953	12	0.533
Piccolo	80/128	64	25/31	432	237	237
KTANTAN	80	32/48/64	254	462–802	–	Low
ASCON	128	–	–	–	–	1000
QARMA	128/256	64/128	3	–	–	Very high
SAT_Jo	80	64	31	1167	1270	14.9

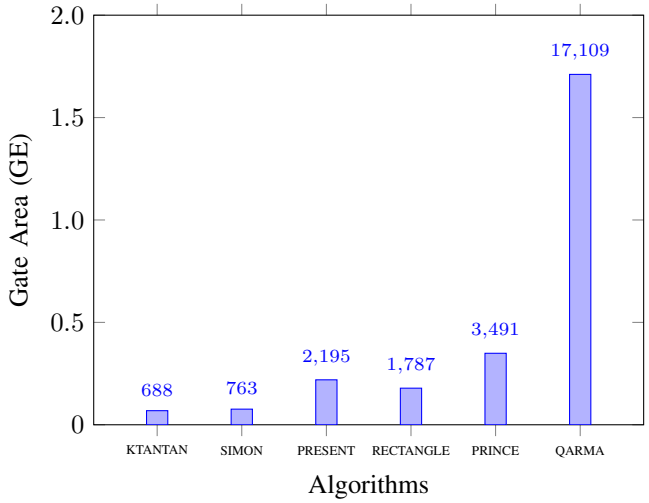

Fig. 2. Gate area (GE) comparison of lightweight block ciphers.

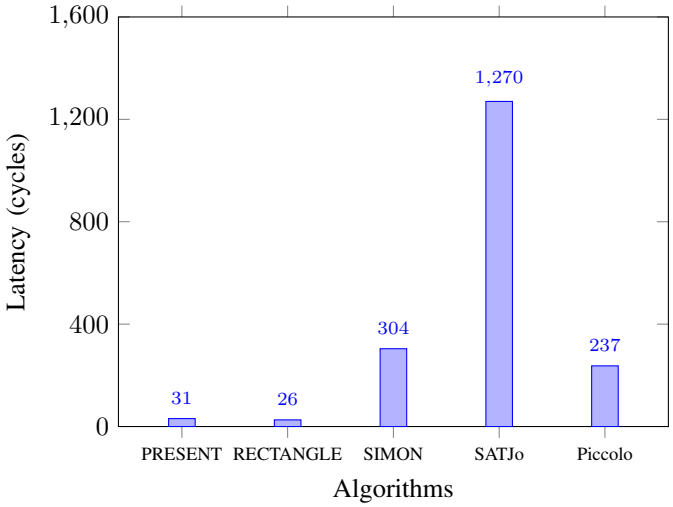

Fig. 3. Latency comparison of lightweight ciphers.

III. Evaluation of the Performance of Lightweight Block Ciphers in Different Domains

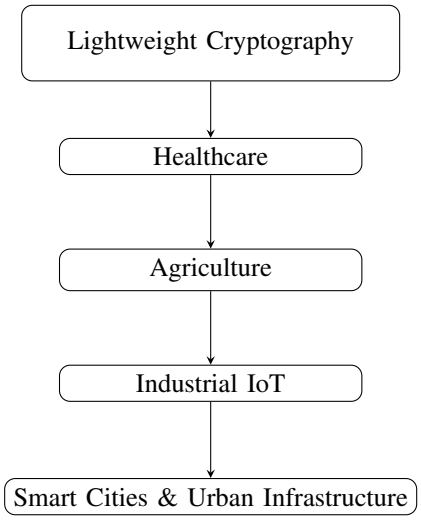

Fig. 4. IoT Domains and Their Security Requirements

A. *Agriculture*

In smart agriculture, IoT devices such as soil sensors, irrigation controllers, and weather-monitoring nodes operate in outdoor environments where power and hardware resources are extremely limited. These devices must transmit data securely while running on small batteries or solar units, making lightweight cryptography essential. Ciphers like PRESENT and SIMON are suitable because of their low gate area and energy efficiency, allowing long-term field deployment. For applications requiring faster responses—such as automated irrigation or drone-based monitoring—algorithms like RECTANGLE and PRINCE offer higher throughput with minimal latency. By using lightweight ciphers, agricultural IoT systems maintain secure communication without affecting device lifetime or system performance.

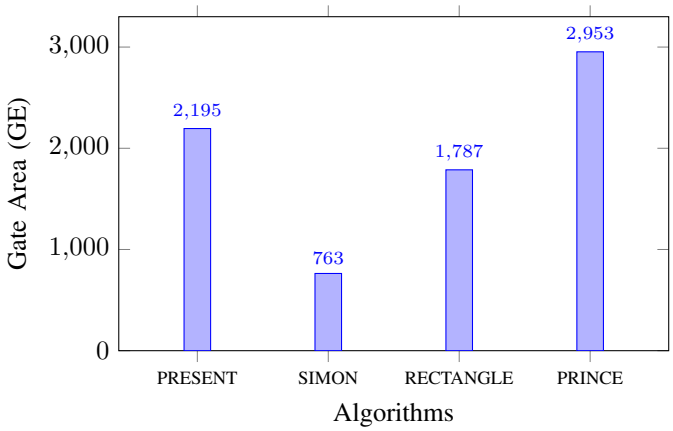

Fig. 5. Gate area comparison for smart agriculture.

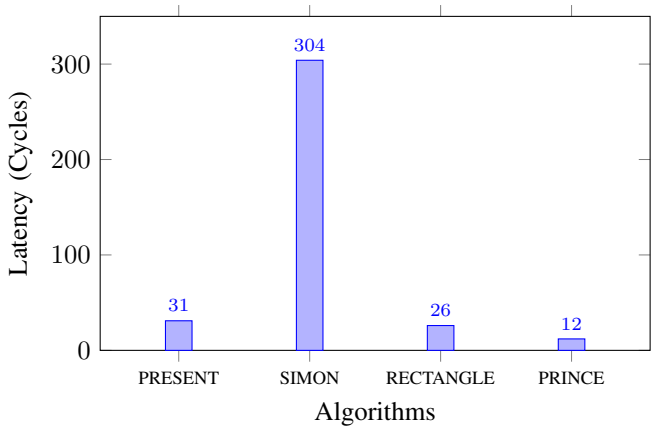

Fig. 6. Latency comparison for smart agriculture.

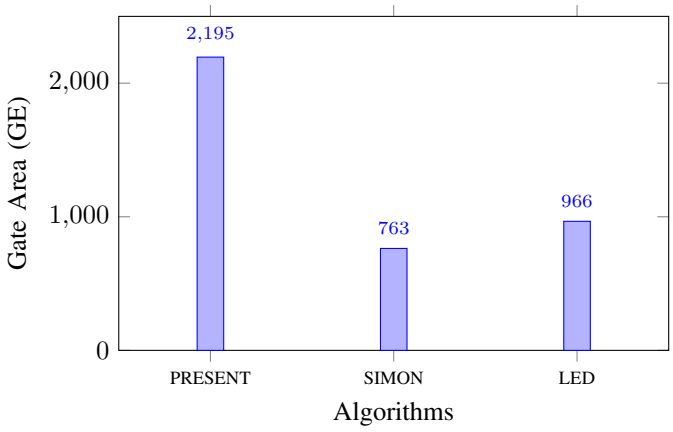

Fig. 8. Gate area comparison for healthcare IoT.

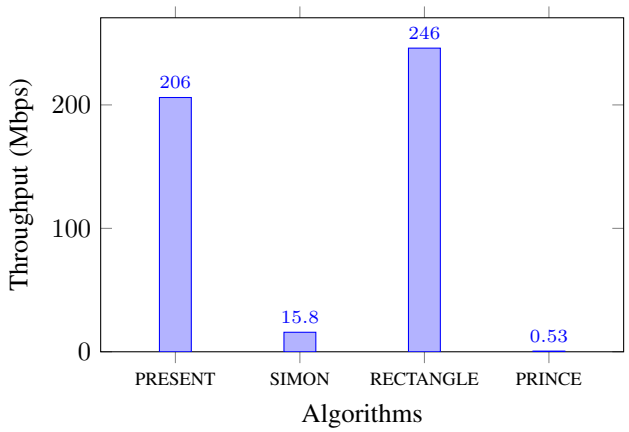

Fig. 7. Throughput Comparison for Smart Agriculture

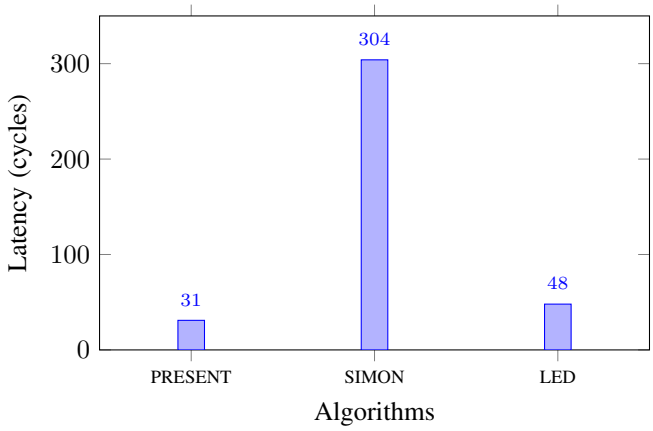

Fig. 9. Latency comparison for healthcare IoT.

B. *Healthcare*

IoT-based healthcare systems rely heavily on wearable sensors, remote diagnostic units, and continuous patient monitoring devices that must function reliably with limited energy and computational resources. These medical sensors constantly generate information such as heart rate, blood pressure, glucose levels, and emergency alerts, all of which require secure transmission to prevent unauthorized access or manipulation. However, traditional cryptographic methods impose high computational overhead, making them unsuitable for battery-operated medical devices. Lightweight cryptographic algorithms address this need by providing fast, low-power, and memory-efficient security while maintaining the confidentiality and integrity of sensitive patient data. Ciphers such as PRESENT, SIMON, and LED are frequently adopted because they offer compact hardware footprints and strong resistance against common attacks, enabling secure medical communication without compromising device longevity or real-time performance.

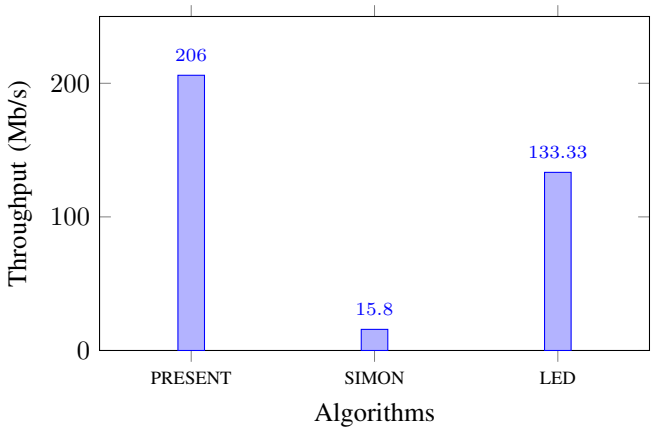

Fig. 10. Throughput comparison for healthcare IoT.

C. *Smart Cities and Urban Infrastructure*

Smart cities integrate a wide range of connected systems—such as intelligent traffic signals, smart grids, environmental monitoring units, and public safety sensors—to support efficient urban management. These devices often operate autonomously in large-scale networks, where maintaining

low latency and reliability is essential for uninterrupted city services. The high density of interconnected devices increases the attack surface, making secure communication a critical requirement. Lightweight cryptography provides an efficient solution for safeguarding sensor data, control messages, and automated decision-making systems in smart cities, where power consumption and hardware space are major constraints. Algorithms like PRINCE, RECTANGLE, and PRESENT are widely considered effective for these environments because they deliver high throughput, low latency, and reduced gate area, making them suitable for real-time city-wide deployments such as smart lighting, traffic monitoring, and energy distribution systems.

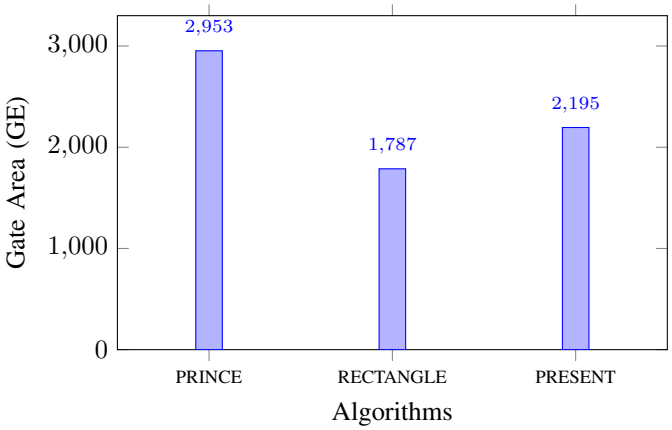

Fig. 11. Gate area comparison for smart city applications.

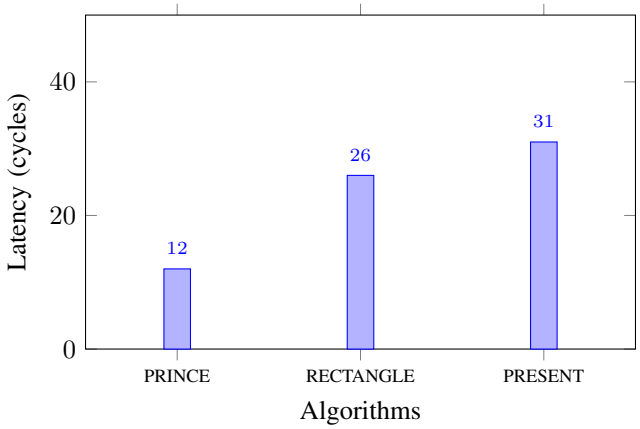

Fig. 12. Latency comparison for smart city applications.

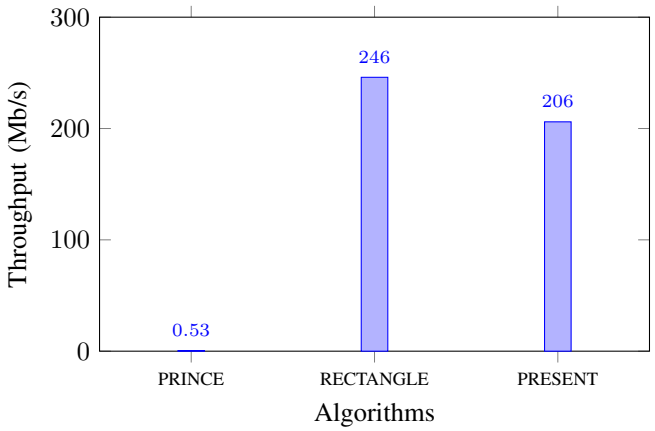

Fig. 13. Throughput comparison for smart city applications.

D. *Industrial IoT (IIoT)*

Industrial IoT environments include factory sensors, robotic controllers, programmable logic controllers (PLCs), and predictive maintenance units that continuously exchange operational and safety-critical information. These systems demand encryption techniques that can perform securely under strict timing, energy, and hardware constraints. Delays or weak security in IIoT networks can disrupt manufacturing processes, affect product quality, or cause machine failures. Lightweight cryptography is therefore essential in IIoT, as it provides strong protection while supporting rapid computation and minimal hardware usage. High-performance ciphers such as PRINCE, KTANTAN, and RECTANGLE are commonly preferred because they offer low execution latency and high throughput, making them suitable for real-time automation, industrial communication protocols, and machine-to-machine control. Their optimized design enables secure data exchange without interfering with the responsiveness required in industrial operations.

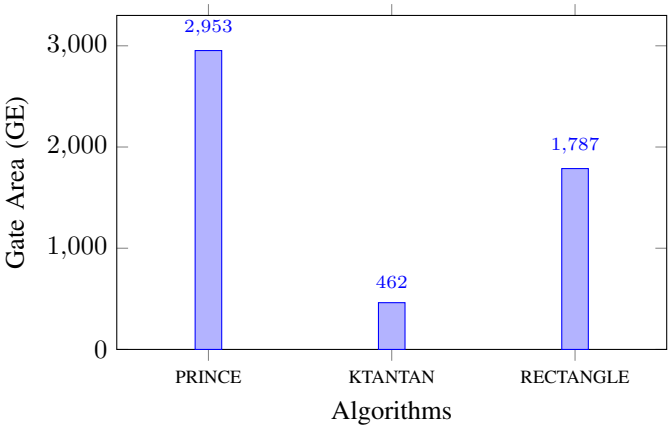

Fig. 14. Gate area comparison for Industrial IoT.

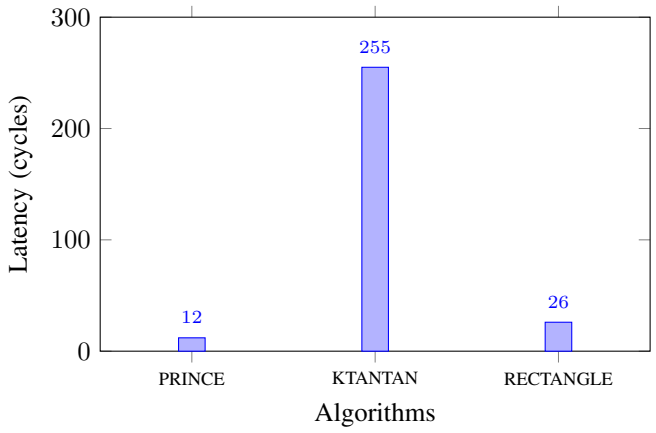

Fig. 15. Latency comparison for Industrial IoT.

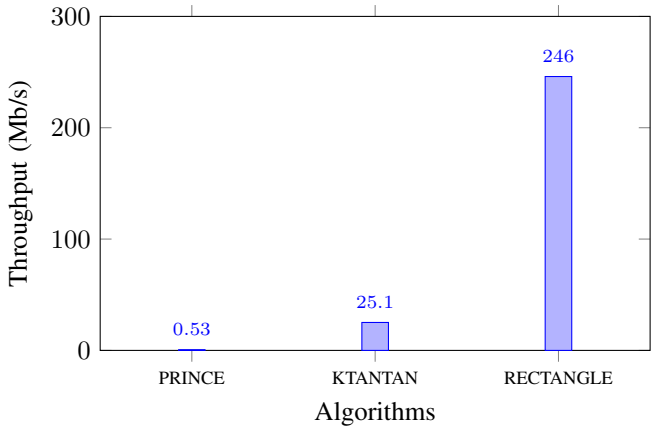

Fig. 16. Throughput comparison for Industrial IoT.

TABLE II
RECOMMENDED LIGHTWEIGHT CIPHERS ACROSS IOT DOMAINS

Domain	Cipher(s)	Selection Criteria
Agriculture	PRESENT, SIMON	Minimum power and low gate cost
Healthcare	LED, PRESENT	Compact hardware; suitable for wearables
Smart Cities	RECTANGLE, PRINCE	High throughput and reduced latency
Industrial IoT	PRINCE, KTANTAN	Fast execution and timing-critical response

IV. RESEARCH GAPS

Although lightweight cryptographic solutions have shown rapid advancements for protecting constrained IoT systems, several challenges still remain unaddressed. Current literature predominantly evaluates algorithms using theoretical performance indicators such as block size, gate area, latency, and throughput, whereas experimental validation on real IoT hardware platforms (e.g., ARM Cortex boards, Arduino, ESP32, and Raspberry Pi) is either minimal or missing. In addition, most implementations are assessed under controlled conditions, overlooking practical limitations such as fluctuating environmental parameters, variable data traffic, intermittent connectivity, and restricted power availability—factors that critically influence agricultural and industrial deployments.

Another major research gap concerns the limited study of resistance against physical and side-channel attacks, which pose significant threats to wearable healthcare devices and IIoT sensors operating in unsecured environments. While authenticated encryption techniques such as ASCON and QARMA are gaining prominence, comprehensive analysis of end-to-end secure frameworks that integrate encryption, key lifecycle management, and device authentication remains inadequate. Moreover, there is currently no standardized benchmarking methodology for selecting cryptographic algorithms based on domain-specific operational constraints, resulting in inconsistent and suboptimal cipher deployment across IoT sectors. These gaps highlight the need for practical, implementation-driven, and context-aware security solutions that align with real-world IoT requirements.

FUTURE RESEARCH DIRECTIONS

Future research should emphasize adaptive and context-aware lightweight cryptography capable of automatically optimizing security operations based on available hardware resources and application demands. Developing standardized benchmarking frameworks that jointly evaluate power consumption, latency, side-channel resistance, and communication cost would enable consistent cipher selection for heterogeneous IoT devices. Furthermore, integrating lightweight security mechanisms with machine-learning driven anomaly detection and exploring post-quantum lightweight ciphers are promising directions for building long-term secure IoT ecosystems.

CONCLUSION

Lightweight cryptography has become an essential security requirement for constrained IoT devices where memory, energy, and processing resources are limited. This review has shown that the selection of a lightweight cipher must be aligned with domain-specific constraints rather than relying solely on general performance metrics. Algorithms such as PRESENT and SIMON are highly suitable for low-power agricultural and healthcare sensors due to their compact hardware footprint, whereas high-speed designs like PRINCE and RECTANGLE provide better efficiency for latency-sensitive applications in smart cities and industrial control systems. The domain-centric comparison clearly demonstrates that no single lightweight cipher satisfies every IoT requirement; instead, optimal security depends on a balance among throughput, gate area, latency, and energy consumption based on the deployment environment.

REFERENCES

[1] A.Bogdanov et al.,"PRESENT: An ultra-lightweight block cipher," in *Proc.Cryptographic Hardware and Embedded Systems (CHES)*,Springer, 2007. [2] A.

Menezes, P. C. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996.

[3] J. Guo, T. Peyrin, A. Poschmann, and M. Robshaw, "The LED block cipher," in *Proc. International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, Springer, 2011, pp. 326–341.
[4] A. Moradi, A. Poschmann, S. Ling, C. Paar, and H. Wang, "Pushing the limits: A compact and threshold implementation of AES," in *Proc. Annual International Conference on the Theory and Application of Cryptology and Information Security (EUROCRYPT)*, Springer, 2011, pp. 69–88. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-20465-4$_6$
[5] J. Guo, T. Peyrin, and A. Poschmann, "The PHOTON family of lightweight hash functions," in *Proc. International Cryptology Conference (CRYPTO)*, Springer, 2011, pp. 222–239.
[6] E. Biham, "New types of cryptanalytic attacks using related keys," *Journal of Cryptology*, vol. 7, no. 4, pp. 229–246, 1994.
[7] J. Guo, T. Peyrin, A. Poschmann, and M. Robshaw, "The LED block cipher," in *Proc. International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, Springer, 2011, pp. 326–341. (Note: appears again in original, kept once.)
[8] W. Zhang et al., "RECTANGLE: A bit-slice lightweight block cipher suitable for multiple platforms," *Science China Information Sciences*, vol. 58, no. 12, pp. 1–15, 2015.
[9] M. R. Albrecht et al., "Block ciphers: Focus on the linear layer (feat. PRIDE)," in *Proc. International Cryptology Conference (CRYPTO)*, Springer, 2014, pp. 57–76.
[10] J. Borghoff et al., "PRINCE: A low-latency block cipher for pervasive computing applications," in *Proc. ASIACRYPT: International Conference on the Theory and Application of Cryptology and Information Security*, Springer, 2012, pp. 208–225. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-34961-4$_1$4
[11] L. Batina et al., "Dietary recommendations for lightweight block ciphers: Power, energy, and area analysis," in *Proc. International Workshop on RFID Security and Privacy Issues (RFIDSec)*, Springer, 2013, pp. 103–112.
[12] K. Shibutani et al., "Piccolo: An ultra-lightweight block cipher," in *Proc. International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, Springer, 2011, pp. 342–357.
[13] C. De Canniere, O. Dunkelman, and M. Knežević, "KATAN and KTANTAN: Small and efficient hardware-oriented block ciphers," in *Proc. Cryptographic Hardware and Embedded Systems (CHES)*, Springer, 2009, pp. 272–288.
[14] T. Eisenbarth et al., "Compact implementation and performance evaluation of block ciphers in ATtiny devices," in *Proc. AFRICACRYPT: International Conference on Cryptology in Africa*, Springer, 2012, pp. 172–187.
[15] L. Wei et al., "Improved meet-in-the-middle cryptanalysis of KTANTAN," in *Proc. Australasian Conference on Information Security and Privacy (ACISP)*, Springer, 2011, pp. 433–438.
[16] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Ascon v1.2," *CAESAR Competition Submission*, 2016.
[17] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Cryptanalysis of ASCON," in *Proc. CT-RSA: Cryptographer's Track at the RSA Conference*, Springer, 2015, pp. 371–387.
[18] R. Avanzi et al., "The QARMAv2 family of tweakable block ciphers," *IACR Transactions on Symmetric Cryptology*, vol. 2023, no. 3, pp. 25–73, 2023.
[19] R. Avanzi, "The QARMA block cipher family," *IACR Transactions on Symmetric Cryptology*, vol. 2017, no. 1, pp. 4–44, 2017.
[20] Arm Community, "Armv8-A architecture: 2016 additions," 2016. Available: https://community.arm.com
[21] R. Zong and X. Dong, "Meet-in-the-middle attack on QARMA block cipher," *IACR ePrint Archive*, Report 2016/1160, 2016. Available: https://eprint.iacr.org/2016/1160
[22] J. Xu, "Qarma64," GitHub Repository, 2022. Available: https://github.com/Phantom1003/QARMA64
[23] M. J. R. Shantha and L. Arockiam, "Sat$_{JO}$: $An enhanced lightweight block cipher for IoT,"$ $in *$ $Proc. International Conference on Intelligent Computing and Control$
[24] T. T. K. Hue, T. M. Hoang, and D. Tran, "Chaos-based S-box for lightweight block cipher," in *Proc. IEEE International Conference on Communications and Electronics (ICCE)*, 2014, pp. 572–577.