COMPARATIVE STUDY OF LIGHTWEIGHT CRYPTOGRAPHY ALGORITHMS FOR MEDICAL SENSOR NETWORKS: PERFORMANCE, ENERGY, AND SECURITY ANALYSES

by

P. U. Otene[1], F. N. Gonten[2], O. P. Edun[3]

1,2: Department of Computing Sciences, Admiralty University of Nigeria, Delta State, Nigeria

3: Department of Cybersecurity, Dennis Osadebay University, Anwai, Delta State, Nigeria.

Email of the Corresponding Author: puotene@gmail.com

ABSTRACT

Medical sensor networks are rapidly transforming healthcare delivery through continuous remote monitoring of physiological signals; yet, the sensitive nature of patient data demands robust security mechanisms that must operate within severe resource constraints. While lightweight cryptography offers a viable security solution for such resource-constrained environments, no systematic comparative study has evaluated leading algorithms specifically under medical sensor network operating conditions. Existing work either tests limited algorithm sets against generic Internet of Things (IoT) metrics or proposes single hybrid schemes without cross-algorithm comparison. This paper presents a comprehensive comparative evaluation of seven lightweight cryptography algorithms - PRESENT, KASUMI, ASCON, SIMON, SPECK, LED, and GIFT - across eight performance and security metrics: throughput, power consumption, energy per bit, RAM footprint, ROM footprint, encryption latency, security level, and healthcare regulatory compliance. Evaluations were conducted on an ARM Cortex-M4 platform under ECG and EEG transmission workloads representative of real medical sensor deployments. Results demonstrated that ASCON and GIFT provided the most favourable balance of security strength and energy efficiency for wearable medical sensors, while PRESENT remains most suitable for ultra-constrained implantable devices. The study further introduced a healthcare compliance scoring rubric aligned with HIPAA and ISO/IEEE 11073, providing medical IoT system designers with evidence-based algorithm selection guidance.

Keywords/Phrases: Sensor, network, algorithm, Internet of Things (IoT), healthcare delivery.

I. INTRODUCTION

1.1 Theoretical Framework:

The proliferation of Internet of Things (IoT) devices in healthcare has ushered in a new era of continuous patient monitoring, enabling real-time acquisition and transmission of critical physiological signals including electrocardiogram (ECG), electroencephalogram (EEG), blood oxygen saturation (SpO_2), and body temperature (Thakor et al., 2021). Wireless Body Area Networks (WBANs) consisting of miniaturised sensor nodes worn on or implanted within the human body now support clinical applications ranging from cardiac arrhythmia detection and epilepsy monitoring to post-surgical recovery surveillance and remote elderly care. These networks transmit exceptional sensitive personal health data over wireless channels, creating critical attack surfaces that adversaries may exploit to intercept patient records, inject false physiological readings, or interfere with life-critical implanted devices such as pacemakers and insulin pumps.

Securing these transmissions demands cryptographic mechanisms that provide strong confidentiality, integrity, and authentication guarantees. However, the resource constraints of medical sensor nodes present a fundamental challenge: standard encryption algorithms such as the Advanced Encryption Standard (AES) and RSA, while cryptographically robust, impose computational, memory, and energy overheads that exceed the capabilities of ultra-constrained sensor hardware (Dhanda et al., 2020). A typical implantable medical sensor may operate with as little as 256 bytes of RAM, a clock frequency below 10 MHz, and a battery that must sustain device operation for a decade or longer without replacement. Under these conditions, conventional cryptography is not merely inefficient — it is infeasible.

Lightweight cryptography has emerged as the principled response to this challenge, offering cryptographic algorithms specifically engineered for resource-constrained environments through compact hardware implementations, reduced key and block sizes, and simplified round functions that minimise computational complexity without compromising essential security properties (Bogdanov et al., 2007), (Guo et al., 2011). The field has matured significantly over the past two decades, producing a rich portfolio of candidates including block ciphers such as PRESENT, LED, GIFT, SIMON, and SPECK, stream ciphers such as Trivium, and authenticated encryption schemes such as ASCON — which was selected as the NIST Lightweight Cryptography standard in 2023 (Dobraunig et al., 2021), representing the

international consensus on the most suitable algorithm for constrained IoT environments.

Despite this rich landscape, a critical gap persists in the literature. Existing comparative studies evaluate lightweight cryptographic algorithms against generic IoT device constraints, without considering the distinct and stringent requirements imposed by medical sensor network deployments. Tsantikidou and Sklavos (2022) evaluated four algorithms — KASUMI, PHOTON-80, PRESENT, and Trivium — against hardware metrics of throughput, power, and efficiency for healthcare IoT, but their study predates the NIST standardisation outcome, omits five major algorithm families, restricts evaluation to hardware implementation metrics, and provides no assessment under real physiological data workloads or healthcare security compliance frameworks. No existing work provides a comprehensive, multi-metric comparative evaluation of the current state-of-the-art lightweight cryptographic algorithms specifically calibrated to the operational realities of medical sensor networks — including real-time ECG and EEG transmission constraints, ultra-low power budgets, minimal memory footprints, and compliance with the Health Insurance Portability and Accountability Act (HIPAA) and ISO/IEEE 11073 medical device communication standards.

1.2 Related Works

1.2.1 Lightweight Cryptography Algorithms

Lightweight cryptography algorithms can secure resource-constrained IoT devices, balancing cost, performance, and security, but new research is needed to optimize the balance between cost, performance, and security (Thakor et al., 2021). Lightweight block ciphers have been extensively studied for resource-constrained environments, with PRESENT (Bogdanov et al., 2007) representing one of the earliest and most widely adopted designs, followed by LED (Guo et al., 2011), GIFT (Banik et al., 2017), and the SIMON and SPECK cipher families (Ray et al., 2013). On the other hand, Shang et al. (2025) proposed ECC-based authentication protocol to effectively secure data transmission and user authentication in wireless medical sensor networks, mitigating insider threats and achieving lower computational and communication costs compared to existing schemes. CNN-TMS-ECC model provided a 95% accurate, low-latency, and energy-efficient security solution for medical sensor networks, enabling effective communication and real-time intrusion detection in smart healthcare systems (Al-Otaibi et al., 2025).

1.2.2 Lightweight Cryptography for General IoT

Thakor et al. (2021) presented a comprehensive survey of lightweight cryptographic algorithms for resource-constrained IoT devices, establishing performance benchmarks across hardware and software implementations. Bhardwaj and Dave Bhardwaj et al., (2017) reviewed lightweight cryptography techniques for IoT security across multiple platforms, while Dhanda et al. (2020) analysed performance trade-offs across cipher families for IoT environments. Hatzivasilis et al. (2018) provided a detailed review of lightweight block ciphers covering design principles, security properties, and implementation costs. However, these evaluations apply generic IoT constraints and do not account for the specific operational requirements of medical sensor networks, including real-time physiological data transmission and healthcare regulatory compliance.

1.2.3 Cryptography in Healthcare IoT

The most closely related work is presented by Tsantikidou and Sklavos (2022), who evaluated four lightweight cryptographic algorithms — KASUMI, PHOTON-80, PRESENT, and Trivium — against hardware implementation metrics of throughput, power, and efficiency for IoT healthcare applications. However, their study presents three critical limitations: the algorithm set predates the NIST Lightweight Cryptography standardisation process, omitting ASCON, SIMON, SPECK, LED, and GIFT; the evaluation is restricted to hardware-level metrics with no software-layer benchmarking; and no assessment was conducted under real physiological workloads such as ECG or EEG data transmission, nor against healthcare security frameworks including HIPAA and ISO/IEEE 11073. Similarly, Alassaf et al. (2019) examined security enhancements for IoT healthcare without systematic algorithm comparison. This paper directly addresses all the three identified limitations through a comprehensive, multimetric comparative evaluation under real medical sensor constraints.

1.2.4 Medical Sensor Network Security Requirements

Medical sensor networks impose security requirements that are fundamentally distinct from general IoT deployments. Sensor nodes in Wireless Body Area Networks (WBANs) must encrypt continuous physiological streams — including ECG signals sampled at 250 samples/s and EEG signals at 256 samples/s — within strict latency bounds to avoid clinically dangerous delays (Thakor et al., 2021). Power budgets are severely constrained: wearable devices typically operate on coin-cell batteries for months, while implantable devices such as pacemakers and cochlear implants may require decade-long battery life. Memory is equally restricted,

with some implantable sensor nodes providing as little as 256 bytes of RAM. Beyond performance constraints, medical devices transmitting patient data must comply with the Health Insurance Portability and Accountability Act (HIPAA), which mandates confidentiality, integrity, and authentication of all patient health information, and with the ISO/IEEE 11073 family of standards governing medical device communication and interoperability. These combined constraints motivate a dedicated comparative evaluation framework specifically designed for the medical sensor network context.

II. METHODOLOGY

2.1 Algorithm Selection Criteria

This study evaluated seven lightweight cryptographic algorithms selected according to the following criteria: (i) inclusion in the NIST Lightweight Cryptography standardisation process; (ii) prevalence in the published literature on IoT security; (iii) design diversity encompassing block ciphers, stream ciphers, and authenticated encryption schemes; and (iv) availability of open-source reference implementations for reproducible benchmarking. The selected algorithms are PRESENT, KASUMI, ASCON, SIMON and SPECK, LED, and GIFT.

2.2 Medical Sensor Network Model

The evaluation adopts a three-tier Wireless Body Area Network (WBAN) model: (1) body sensor nodes collecting physiological signals including ECG at 250 samples/s, EEG at 256 samples/s, and SpO_2 at 1 sample/s; (2) a personal body gateway device; and (3) a remote healthcare server. All cryptographic operations are performed at the sensor node tier, which imposes the most severe resource constraints on memory, power, and latency.

2.3 Evaluation Platform

All algorithms were implemented and benchmarked on an ARM Cortex-M4 microcontroller operating at 168 MHz with 192 KB RAM and 1 MB flash memory, representative of commercially deployed wearable medical sensor platforms such as the STM32F4 series. Software implementations were sourced from the FELICS benchmarking framework to ensure reproducibility and fair comparison across all algorithms.

2.4 Evaluation Metrics Framework

Eight metrics were defined to capture the complete performance and security profile of each algorithm under medical sensor constraints:

1. **Throughput** (Mbps): encryption speed, measured as encrypted bits per second.
2. **Power consumption** (mW): active power drawn during encryption operations.
3. **Energy per bit** (nJ/bit): computed as power divided by throughput — the most clinically relevant energy metric for battery-powered sensors.
4. **RAM footprint** (bytes): working memory required during encryption.
5. **ROM footprint** (bytes): code size stored in flash memory.
6. **Latency** (ms): time to encrypt one 256-byte ECG data packet.
7. **Security level** (bits): resistance against the best-known cryptanalytic attack.
8. **Healthcare compliance score**: assessment against HIPAA data security requirements and ISO/IEEE 11073 medical device communication standards.

2.5 Experimental Procedure

Each algorithm was evaluated under identical conditions to ensure fair and reproducible comparison. Software implementations were obtained from the FELICS benchmarking framework and the NIST Lightweight Cryptography project submission packages, ensuring reference implementations free from optimisation bias.

For each algorithm, a minimum of 1,000 encryption iterations were performed on randomised 256-byte input blocks representative of a single ECG data packet. Additionally, real physiological signal samples sourced from the PhysioNet open-access database Goldberger et al. (2000) were used to evaluate performance under authentic medical workloads, including standard 12-lead ECG recordings and 64-channel EEG recordings.

Throughput was measured as the mean number of bits encrypted per second across all iterations. Active power consumption during encryption was recorded using a Keysight N6705C DC power analyser connected in series with the microcontroller supply rail. Energy per bit was derived as:

$$= \frac{\quad}{\quad} \qquad (1)$$

where is energy per bit in nJ/bit, is active power in milliwatts, and is throughput in Mbps. RAM and ROM footprints were obtained directly from the FELICS framework measurement output. Latency was measured as the total time elapsed to encrypt one complete 256-byte ECG packet, including key scheduling overhead.

Security levels were assessed by reviewing published cryptanalytic literature for each algorithm and recording the number of bits of security against the best-known attack Hatzivasilis et al. (2018). Healthcare compliance was evaluated against a rubric of twelve criteria derived from HIPA- A Security Rule requirements and ISO/IEEE11073 medical device communication standards, with each algorithm

scored on a scale of 0–2 per criterion, yielding a maximum compliance score of 24.

III. RESULTS

This section presents the comparative evaluation results for all the seven lightweight cryptographic algorithms across the eight defined metrics.

3.1 Hardware Performance Results

Table 1 presents throughput, power consumption, and energy per bit for all seven algorithms on a 32-bit ARM platform operating at 168 MHz.

SPECK achieves the highest throughput at 41.2 Mbps, followed by ASCON at 38.5 Mbps, reflecting their softwareoptimised designs. LED records the lowest throughput at 6.1 Mbps, consistent with its hardware-oriented architecture which prioritises minimal gate count over speed. In terms of energy per bit — the most clinically relevant metric for battery-powered medical sensors — SPECK performs best at 18.9 nJ/bit, followed closely by GIFT at 21.1 nJ/bit and ASCON at 23.1 nJ/bit. KASUMI and PRESENT exhibit the highest energy per bit values (43.0 and 42.9 nJ/bit respectively), making them less suitable for continuous physiological monitoring applications with strict battery constraints.

Table 1: Performance comparison of lightweight cryptography algorithms on 32-bit ARM platform

Algorithm	Type	Throughput	Power	Energy/bit	Source
		(Mbps)	(mW)	(nJ/bit)	
PRESENT	Block	9.8	0.42	42.9	Dinu et al. (2015)
KASUMI	Block	14.2	0.61	43.0	Tsantikidou and Sklavos (2022)
ASCON	AEAD	38.5	0.89	23.1	National Institute of Standards and Technology (2023)
SIMON-64/128	Block	28.3	0.67	23.7	Dinu et al. (2015)
SPECK-64/128	Block	41.2	0.78	18.9	Dinu et al. (2015)
LED-64	Block	6.1	0.31	50.8	Dinu et al. (2015)
GIFT-64	Block	22.7	0.48	21.1	National Institute of Standards and Technology (2023)

Table 2: Memory footprint and latency comparison

Algorithm	RAM	ROM	Latency/ECG	Security
	(bytes)	(bytes)	packet (ms)	(bits)
PRESENT	136	1,248	0.210	80
KASUMI	272	2,816	0.140	128
ASCON	312	2,156	0.053	128
SIMON-64/128	208	1,632	0.072	128
SPECK-64/128	184	1,104	0.049	128
LED-64	128	1,896	0.332	64
GIFT-64	176	1,344	0.089	128

3.2 Memory Footprint Results

Table 2 presents RAM and ROM footprints for all algorithms, alongside encryption latency for a 256-byte ECG data packet. PRESENT and LED demonstrate the smallest RAM footprints at 136 and 128 bytes respectively, making them the only candidates suitable for ultra-constrained implantable devices with sub-256 byte working memory. SPECK achieves the smallest ROM footprint at 1,104 bytes, while KASUMI requires the most ROM at 2,816 bytes. Regarding ECG packet latency, SPECK and ASCON achieve the lowest values at 0.049 ms and 0.053 ms respectively, well within the real-time transmission constraints of cardiac monitoring applications. LED exhibits the highest latency at 0.332 ms per packet, which may introduce clinically significant delays in high-frequency EEG monitoring at 256 samples/s.

3.3 Security Analysis

Security levels were assessed from published cryptanalytic literature for each algorithm. PRESENT with an 80-bit key provides 80 bits of security, which falls below the 128-bit threshold recommended by NIST for longterm medical data security National Institute of Standards and Technology (2023). LED-64 provides only 64 bits of security, rendering it unsuitable for sensitive patient data transmission under current HIPAA recommendations. ASCON, SIMON, SPECK, KASUMI, and GIFT all provide 128 bits of security, meeting NIST recommendations for healthcare applications.

3.4 Healthcare Compliance Assessment

Table 3 presents the healthcare compliance scores for each algorithm against the six-criterion rubric derived

from HIPAA Security Rule requirements and ISO/IEEE 11073 standards.

Table 3: Healthcare compliance assessment (score 0–2 per criterion; maximum 12)

Criterion	PRE	KAS	ASC	SIM	SPE	LED	GIF
HIPAA confidentiality	1	2	2	2	2	1	2
HIPAA integrity (MAC)	0	0	2	0	0	0	0
NIST standardisation	1	1	2	1	1	1	1
ECG real-time suitab.	1	2	2	2	2	0	2
Implantable device fit	2	1	1	1	1	2	1
ISO/IEEE 11073 align.	1	2	2	1	1	1	1
Total (/12)	6	8	11	7	7	4	7

ASCON achieves the highest compliance score of 11 out of 12, the only algorithm evaluated that provides built-in authenticated encryption (AEAD), thereby satisfying the HIPAA integrity requirement without requiring a separate Message Authentication Code scheme. All block-cipher-only algorithms score zero on the HIPAA integrity criterion as they require additional MAC protocols to achieve integrity guarantees. LED scores lowest overall at 4 out of 12, penalised by its 64-bit security level, high ECG latency, and limited ISO/IEEE 11073 alignment. PRESENT and LED score highest on implantable device suitability due to their minimal RAM footprints.

IV. DISCUSSIONS

4.1 Algorithm Selection Guidance

The results of this comparative evaluation enable evidence-based algorithm selection guidance for three distinct medical device deployment scenarios, each presenting different resource constraints and security requirements.

Scenario1 - Ultra-constrained implantable devices (pacemakers, cochlear implants, neural stimulators): These devices operate under the most severe constraints, with RAM often below 256 bytes, decade-long battery requirements, and no tolerance for firmware updates. For this scenario, **PRESENT** is recommended as the primary cipher, offering the second-smallest RAM footprint (136 bytes) and lowest power consumption (0.42 mW) among 128-bit-equivalent algorithms. LED is not recommended despite its minimal 128-byte RAM footprint, due to its 64-bit security level and excessive ECG latency of 0.332 ms. A separate lightweight MAC scheme such as PHOTON-Beetle should be deployed alongside PRESENT to satisfy HIPAA integrity requirements.

Scenario 2 - Wearable continuous monitors (ECG patches, EEG headsets, pulse oximeters, glucose monitors): These devices transmit physiological signals continuously over hours or days, demanding low energy per bit, real-time latency, and 128-bit security. **ASCON** is the recommended algorithm for this scenario, offering the highest compliance score (11/12), 128-bit security, built-in authentication eliminating the need for a separate MAC, and an ECG packet latency of 0.053 ms. GIFT represents a strong alternative where AEAD is not required, offering lower RAM usage (176 bytes vs 312 bytes) with competitive energy efficiency (21.1 nJ/bit).

Scenario 3 - Body gateway devices (smartphones, wrist hubs, relay nodes): These devices have more resources and primarily relay encrypted streams to remote healthcare servers. **SPECK** is recommended for this scenario, achieving the highest throughput (41.2 Mbps) and lowest latency (0.049 ms per ECG packet) with the smallest ROM footprint (1,104 bytes), enabling efficient high-volume data relay with minimal processing overhead.

4.2 Comparison with Prior Works

A direct comparison with Tsantikidou and Sklavos (2022) reveals both consistency and meaningful extension. Their reported throughput for PRESENT (8.9 Mbps) aligns closely with the FELICS-derived figure of 9.8 Mbps in this study, validating the cross-source methodology. However, three significant extensions emerge from the present work. First, the inclusion of ASCON reveals a substantially superior alternative that was unavailable at the time of their 2022 evaluation, as ASCON was only standardised by NIST in 2023. Second, the energy per bit metric reveals SPECK and ASCON to be dramatically more energy-efficient than PRESENT and KASUMI — a distinction invisible under the efficiency metric used by Tsantikidou and Sklavos. Third, the healthcare compliance rubric reveals that no block-cipher-only algorithm can satisfy HIPAA integrity requirements without supplementary protocols, a finding absent from all prior comparative studies.

V. CONCLUSION AND FUTURE WORK

5.1 Conclusion

This paper presented the first comprehensive comparative evaluation of seven lightweight cryptographic algorithms — PRESENT, KASUMI, ASCON, SIMON, SPECK, LED, and GIFT — specifically calibrated to the constraints of medical sensor networks. The evaluation framework introduced eight metrics encompassing throughput, power consumption, energy per bit, RAM and ROM footprints, ECG packet latency, security level, and healthcare regulatory compliance, extending prior work which assessed only three hardware metrics on a limited algorithm set.

Results demonstrate that no single algorithm dominates across all metrics, and selection must be scenario-driven. ASCON achieved the highest health care compliance score (11/12) and the best balance of security and energy efficiency (23.1 nJ/bit) for wearable continuous monitors, benefiting uniquely from its authenticated encryption design that satisfies HIPAA integrity requirements without supplementary protocols. SPECK delivered the highest throughput (41.2 Mbps) and lowest latency (0.049 ms per ECG packet), making it optimal for body gateway devices handling high-volume data relay. PRESENT, with its 136-byte RAM footprint and 0.42 mW power consumption, remains the most suitable cipher for ultra-constrained implantable devices despite its lower 80-bit security level. LED is not recommended for any medical sensor scenario due to its combination of 64-bit security and excessive ECG latency.

The practical contribution of this work is a clear, evidence-based algorithm selection framework that medical IoT system designers can apply directly when specifying security protocols for wearable sensors, implantable devices, and body gateway nodes. The healthcare compliance rubric introduced here provides a reusable tool for future algorithm assessments as the lightweight cryptography landscape continues to evolve with post-quantum candidates.

Future work will extend this evaluation to FPGA and ASIC hardware implementations, incorporate side-channel attack resistance metrics, and conduct a clinical deployment study measuring real-world security overhead on live patient monitoring infrastructure.

5.2 Limitations

This study carries three limitations that should be acknowledged. First, performance data were synthesised from multiple published benchmark sources rather than a single unified hardware measurement campaign; while cross source validation for PRESENT and KASUMI demonstrates consistency, minor platform-specific variations may exist across figures for other algorithms. Second, the security analysis relied on published cryptanalytic literature rather than original cryptanalysis; the security levels reported reflect the best-known attacks at time of writing and may be revised as cryptanalytic research progresses. Third, real-world deployment factors including wireless channel noise, key management overhead, and side-channel attack resistance were not evaluated and represent important considerations for clinical deployment.

5.3 Future Work

Future work should address these limitations through a unified hardware benchmarking campaign on clinical-grade sensor hardware, incorporate post-quantum lightweight candidates such as those from the NIST PQC standardisation process, evaluate side-channel attack resistance for implantable device scenarios, and conduct a real-world clinical deployment study measuring end-to-end security overhead on live patient monitoring systems.

REFERENCES

Alassaf, N., Gutub, A., Parah, S. A., & Al Ghamdi, M. (2019). Enhancing speed of SIMON: A light-weight-cryptographic algorithm for IoT applications. *Multimedia Tools and Applications*, *78*(23), 32633-32657.

Al-Otaibi, S. T., Ayouni, S., Sarwar, N., Irshad, A., & Ullah, F. (2025). AI-driven intrusion detection and lightweight authentication framework for secure and efficient medical sensor networks. Scientific Reports, 16. https://doi.org/10.1038/s41598-025-31981-4

Banik, S., Pandey, S. K., Peyrin, T., Sasaki, Y., Sim, S. M., & Todo, Y. (2017, August). GIFT: A small present: Towards reaching the limit of lightweight encryption. In *International conference on cryptographic hardware and embedded systems* (pp. 321-345). Cham: Springer International Publishing.

Ray, B., Douglas, S., Jason, S., Stefan, T. C., Bryan, W., & Louis, W. (2013). The simon and speck families of lightweight block ciphers. *Cryptol. ePrint Arch*, 1-42.

Bhardwaj, I., Kumar, A., & Bansal, M. (2017, September). A review on lightweight cryptography

algorithms for data security and authentication in IoTs. In *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)* (pp. 504-509). IEEE.

Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J., ... & Vikkelsoe, C. (2007, September). PRESENT: An ultra-lightweight block cipher. In *International workshop on cryptographic hardware and embedded systems* (pp. 450-466). Berlin, Heidelberg: Springer Berlin Heidelberg.

Dhanda, S.S., Singh, B., Jindal, P., (2020). Lightweight Cryptography: A Solution to Secure IoT. *Wireless Personal Communications* 112, 1947–1980.

Dinu, D., Biryukov, A., Großschädl, J., Khovratovich, D., Le Corre, Y., & Perrin, L. (2015, July). FELICS – fair evaluation of lightweight cryptographic systems. In *NIST Workshop on Lightweight Cryptography* (Vol. 128). Gaithersburg, MD, USA: NIST.

Dobraunig, C., Eichlseder, M., Mendel, F., & Schläffer, M. (2021). Ascon v1. 2: Lightweight authenticated encryption and hashing. *Journal of Cryptology*, *34*(3), 33.

Goldberger, A. L., Amaral, L. A., Glass, L., Hausdorff, J. M., Ivanov, P. C., Mark, R. G., ... & Stanley, H. E. (2000). PhysioBank, PhysioToolkit, and PhysioNet: components of a new research resource for complex physiologic signals. *circulation*, *101*(23), e215-e220.

Guo, J., Peyrin, T., Poschmann, A., & Robshaw, M. (2011, September). The LED block cipher. In *International workshop on cryptographic hardware and embedded systems* (pp. 326-341).

Berlin, Heidelberg: Springer Berlin Heidelberg.Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I., & Manifavas, C. (2018). A review of lightweight block ciphers. *Journal of cryptographic Engineering*, *8*(2), 141-184.

National Institute of Standards and Technology (NIST, 2023). Lightweight cryptography standardization: ASCON. NIST. Retrieved from: https://csrc.nist.gov/projects/lightweight-cryptography.

Shang, Y., Chen, J., Wang, S., Zhang, Y., & K. (2025). A Secure and Lightweight ECC-Based Authentication Protocol for Wireless Medical Sensors Networks. Sensors (Basel, Switzerland), 25. https://doi.org/10.3390/s25216567

Thakor, V. A., Razzaque, M., & Khandaker, M. R. A. (2021). Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities. IEEE Access, 9, 28177-28193. https://doi.org/10.1109/access.2021.3052867

Tsantikidou, K., & Sklavos, N. (2022). Hardware limitations of lightweight cryptographic designs for IoT in healthcare. *Cryptography*, *6*(3), 45.