International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Securing the Edge: An Analysis of Lightweight Cryptography for Resource-Constrained Network Devices

Naresh Kalimuthu

naresh.kalimuthu@gmail.com

Abstract:
The security of the Internet of Things (IoT) depends not only on strong network protocols but also on the physical security of endpoint devices. While higher-level systems handle access policies, edge devices often with less than 10 KB of RAM need specialized cryptographic primitives to safeguard data from physical extraction and tampering. This paper examines the "Lightweight Cryptography (LWC) Triad": balancing algorithm size, vulnerability to physical attacks, and the high cost of countermeasures. It criticizes the industry's focus on raw gate counts, arguing that "mask-ability," the ease of defending a cipher against side-channel attacks, is a better metric. By comparing the National Institute of Standards and Technology (NIST) approved ASCON standard with the hardware-optimized GIFT-COFB, the paper offers strategic guidance for protecting Class 0 and Class 1 devices. It highlights the urgent research gap in Post-Quantum Lightweight Cryptography (PQLWC) needed to secure long-term infrastructure against future threats.

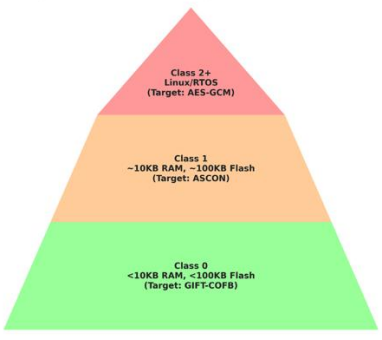
Keywords: Lightweight Cryptography (LWC), ASCON, Side-Channel Analysis (SCA), Class 0 Devices, NIST SP 800-232, Post-Quantum Cryptography (PQC).

I. INTRODUCTION

A. The (Internet Of Things)IoT Resource Landscape

The IoT ecosystem is often mistakenly seen as a uniform network of "smart" devices. In fact, it consists of layered levels. At the lowest level are "constrained nodes," officially defined by the IETF (RFC 7228), which have severe resource restrictions. This paper specifically examines Class 0 devices (such as passive RFID tags and sensor motes with less than 10 KB RAM and 100 KB Flash) and Class 1 devices (around 10 KB RAM, 100 KB Flash). Unlike powerful Electronic Control Units (ECUs) that can run standard IP stacks, these devices cannot support traditional security protocols without depleting their energy or memory. Recent surveys show that, despite the growth of IoT, many edge devices remain at risk due to the resource-intensive nature of legacy cryptographic standards.

Diagram A: The IoT Resource Pyramid (Class 0 vs Class 1)



B. The "Heavy" Legacy

For many years, the Advanced Encryption Standard (AES) has been considered the benchmark for confidentiality. However, the current need for Authenticated Encryption with Associated Data (AEAD) highlights AES's limitations in constrained environments. The typical mode, AES-GCM (Galois/Counter Mode), depends on GHASH for authentication, which operates in a binary Galois field. This process requires a complex, resource-heavy multiplier circuit that is not related to the AES core. Implementing these doubles the hardware area or cycle time, making AES-GCM too resource-intensive for Class 0 devices, where every transistor's power consumption matters. Recent IETF drafts recognize these issues and suggest improvements, such as GCM-SST (Galois Counter Mode with Secure Short Tags), to address tag truncation and enhance security, but hardware overhead issues still hinder the smallest devices.

C. The NIST Standardization Milestone

Recognizing this gap, the National Institute of Standards and Technology (NIST) initiated a multi-year standardization effort to identify a successor to AES suitable for constrained environments. This effort culminated in 2023 with the selection of the ASCON family, officially published as NIST SP 800-232 in August 2025. ASCON signifies a significant shift, transitioning from traditional block ciphers to permutation-based cryptography that includes native AEAD (Authenticated Encryption with Associated Data) and hashing functionalities with a small footprint. This standardization establishes a benchmark for hardware accelerators, promoting compatibility among vendors.

D. Strategic Bridge

While advanced architectures such as Blockchain-managed Attribute-Based Encryption secure data flow and access policies among stakeholders, the integrity of the device itself depends on lightweight primitives that can withstand physical extraction. If the physical edge is compromised, the data entering the blockchain ecosystem is corrupted from the start. This paper focuses on the essential physical layer that enables secure data ingestion for protocols such as OSCORE.

II. THE CORE PROBLEM: THE " LIGHTWEIGHT CRYPTOGRAPHY (LWC) TRIAD"

Designing for the edge requires solving a triad of interconnected challenges that do not exist in server or desktop environments.

A. Challenge 1: The Design Tension

The first challenge involves balancing cryptographic security margins with the implementation footprint. In hardware (ASIC/FPGA), footprint is measured in Gate Equivalents (GE), whereas in software, it is measured in terms of RAM and ROM usage. Unlike ABE(*Attribute-Based Encryption*), which is inherently computationally intensive for supporting complex policies, Lightweight Cryptography (LWC) focuses on minimizing circuit area down to fractions of a millimeter to cut costs and power consumption. The key research difficulty is decreasing the number of logic gates without significantly lowering the cipher's algebraic degree, which could make it susceptible to linear or differential cryptanalysis.

B. Challenge 2: The Physical Threat Model

The threat model for an edge device is unique: the attacker is assumed to have physical access. This proximity allows for two devastating classes of attacks:

1) Side-Channel Analysis (SCA): By observing power usage or electromagnetic (EM) emissions during cryptographic processes, an attacker can statistically link physical leaks to internal secret states to determine the key. Recent research has shown that Deep Learning-based SCA attacks can successfully target unprotected ASCON implementations, recovering keys with fewer than 24,000 traces.

2) Fault Injection (FA): Active attackers can intentionally cause device errors—through voltage spikes, clock tampering, or lasers—leading to computational faults. Examining these faulty outputs using a method known as Differential Fault Analysis can easily uncover the secret key. Additionally, targeted

attacks such as Statistical Ineffective Fault Analysis (SIFA) have proven effective against LWC candidates that lack specific hardware protection hardening.

C. Challenge 3: The Cost of Countermeasures

The actual expense of a lightweight cipher isn't its basic implementation but the additional costs for protection. Masking (or Threshold Implementation) is the primary defense against Side-Channel Analysis (SCA), which involves splitting sensitive data into multiple random shares. Although linear operations like XOR are inexpensive to mask, non-linear operations such as S-boxes require significantly more area and randomness, increasing the overall size. A small, unprotected cipher can become considerably larger once masked, undermining its "lightweight" advantage.

III. ARCHITECTURAL NIST LWC STANDARDS

A. The "Gate Count Fallacy"

The industry often focuses excessively on raw Gate Equivalents (GE), leading to a "race to the bottom." Nevertheless, relying solely on this metric can be misleading if the costs linked to physical aspects are not taken into account security.

1) AES-GCM Overhead: A compact 8-bit AES encryption core can be built in about 2,400 GE, but adding the GHASH multiplier for GCM mode often increases the total to over 10,000 GE. Additionally, masking the AES S-box, which involves inversion in GF(2^8), is mathematically complex and usually requires a substantial amount of fresh randomness (entropy) per cycle to ensure security, resulting in higher power consumption.

2) Permutation Efficiency: Permutation-based ciphers, such as ASCON, eliminate the need for separate key-scheduling logic and distinct encryption and decryption circuits. This streamlined method minimizes control logic, resulting in a smaller overall system than traditional block cipher modes.

B. Emphasizing the "Mask-ability" Argument

NIST selected ASCON (NIST SP 800-232) because it provides an ideal balance between baseline performance and the "cost of protection."

1) Implementation Metrics: The unprotected hardware implementation of the ASCON permutation core requires approximately 4,700 GE. While this is larger than the smallest block ciphers, it offers comprehensive AEAD and Hashing functionalities in a single module circuit.

2) Ease of Protection (Mask-ability): A main feature of ASCON is its "TI-friendly" 5-bit S-box, with an algebraic degree of 2, allowing for efficient resistance to side-channel attacks. A first-order Threshold Implementation (TI) of ASCON requires approximately 8,000 GE, which is just 3.1 times the cost of the unprotected version. Conversely, masking AES generally incurs much higher costs in area and other resources latency.

3) Vulnerability Mitigation: Unprotected ASCON is vulnerable to Deep Learning SCA, which can be recovered in about 24,000 traces, and SIFA, which can be exploited with approximately 280 faults. However, typical countermeasures, such as the ROCKY implementation, have proven to mitigate these fault-injection risks with significantly less hardware overhead.

C. Focusing on the Target Environment (Class 0)

For Class 0 devices, where even ASCON's 4,700 GE might be too large, GIFT-COFB, a NIST finalist GIFT-COFB represents the height of hardware minimization.

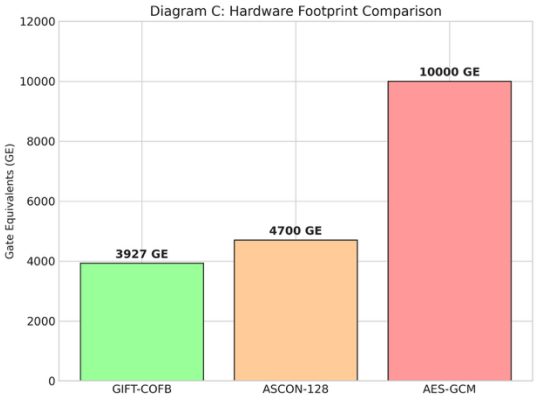
1) Extreme Compactness: An unprotected hardware implementation of GIFT-COFB requires only 3,927 GE. This efficiency is made possible by employing the GIFT-128 block cipher, a refined version of PRESENT, along with the Combined Feedback (COFB) mode.

2) Trade-offs: GIFT-COFB, though smaller, is strictly an authenticated encryption scheme and does not inherently support hashing, unlike ASCON does. This limits its flexibility in protocols that need

signature verification but makes it more suitable for ultra-constrained RFID tags where only basic encryption is necessary.

TABLE I. HARDWARE FOOTPRINT COMPARISON (UNPROTECTED ASIC 65NM)

ALGORITHM	TYPE	FUNCTIONALITY	AREA (GATE EQUIVALENTS)
AES-GCM	BLOCK CIPHER	AEAD	~10,000+ GE (WITH GHASH)
ASCON-128	PERMUTATION	AEAD + HASH	4,700 GE
GIFT-COFB	BLOCK CIPHER	AEAD ONLY	3,927 GE



IV. STRATEGIC RECOMMENDATIONS FOR IMPLEMENTATION

A. The "Mask-ability" Metric

In future hardware designs, engineers should focus on "Mask-ability"—the ability to effectively strengthen a cipher—more than on raw speed.

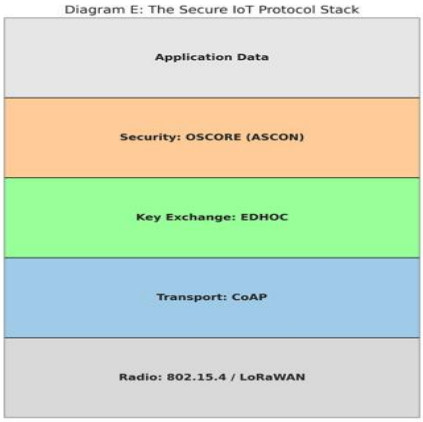
- *Recommendation:* Prioritize algorithms that use low algebraic degree S-boxes (such as ASCON's degree-2 S-box) in environments with high physical attack risks. Higher-degree S-boxes (for example, AES's degree-7) need more shares and additional "fresh randomness" to effectively mask the data securely.
- *Rationale: Generating random bits for masking consumes a lot of energy. A cipher that needs fewer random bits to ensure first-order security will reduce the overall system power consumption, helping to prolong the battery life of Class 1 devices.*

B. Standardization for Interoperability

Adopting NIST SP 800-232 is essential for addressing the fragmentation within the IoT ecosystem.

1) Protocol Integration: Standardization enables ASCON to be seamlessly integrated into lightweight communication protocols. In particular, ASCON is well-suited for the Object Security for Constrained RESTful Environments (OSCORE) protocol (RFC 8613). OSCORE secures CoAP messages at the application layer, providing end-to-end security even when passing through untrusted networks gateways.

2) Key Management: ASCON can be combined with EDHOC (Ephemeral Diffie-Hellman Over COSE), a lightweight protocol for secure key exchange tailored for constrained devices. Together with OSCORE, this combined setup (ASCON + OSCORE + EDHOC) provides a comprehensive, standardized security stack suitable for Class 1 devices, replacing proprietary, often insecure ad hoc solutions.



V. THE NEXT FRONTIER: POST-QUANTUM LWC

A. The "Harvest Now, Decrypt Later" Threat

While ASCON protects against current threats, it depends on traditional security assumptions. IoT devices used in critical infrastructure, such as smart meters and automotive ECUs, often last over 15 years. Attackers can intercept and store encrypted data now, waiting for a future quantum computer capable of breaking the encryption to decrypt it. This risk is especially serious for long-lasting devices that are difficult to update or patch.

B. The Research Gap: RAM Constraints on Class 0 Devices

A significant "Research Gap" exists in Post-Quantum Lightweight Cryptography (PQLWC). The current NIST Post-Quantum Cryptography (PQC) standards are too resource-intensive for Class 0/1 devices.

1) Kyber (ML-KEM) Constraints: The NIST-standardized Kyber-512 (ML-KEM-512) needs about 8–12 KB of RAM solely for storing the polynomial state and executing the Number Theoretic Transform (NTT) operations. This amount surpasses the total RAM available on a Class 0 device (<10 KB).

2) Dilithium (ML-DSA) Constraints: The Dilithium signature scheme features large key sizes and signature data, which pose challenges for the Maximum Transmission Unit (MTU) of low-power radio protocols such as Zigbee or LoRaWAN. Additionally, implementing Dilithium on 8-bit microcontrollers is extremely slow without specialized hardware acceleration.

C. Future Directions

To bridge this gap, future research must focus on:

1) Hardware Acceleration: Implementing PQC solely in software on Class 0 devices is impractical. Hardware accelerators, such as NTT units for polynomial multiplication, are necessary to offload processing and minimize memory usage.

2) Hybrid Schemes: Meanwhile, 'Hybrid' modes that merge ASCON (for quick operation) with a PQC Key Encapsulation Mechanism (for durable key setup) provide a practical transition option, as long as the PQC part can be performed infrequently or delegated to a gateway.

VI. CONCLUSION

Securing the edge requires a comprehensive engineering perspective that balances the algorithmic footprint with the practical realities of physical attacks. Although the "gate count fallacy" encourages designers to opt for the smallest cipher, real security costs are driven by countermeasure overheads like masking. The NIST standardization of ASCON offers a well-balanced, adaptable, and physically hardenable trust anchor, with a 3.1x masking overhead that is much lower than the costs associated with legacy standards. Securing this physical layer with robust Lightweight Wing Control (LWC) provides a strong foundation for dependable, complex, decentralized access control systems. Nonetheless, the impending threat of quantum computing calls for immediate research into hardware-accelerated post-

quantum cryptography (PQC) solutions that can operate within the strict <10 KB RAM constraints of the most limited IoT devices.

REFERENCES:

1. Albrecht, M., Almatrafi, E., Au, M. H., et al. (2022). Round 3 NIST PQC Submissions: Kyber and Dilithium. National Institute of Standards and Technology. **DOI:** 10.6028/NIST.IR.8413
2. Thakor, Vishal & Razzaque, Mohammad Abdur & Khandaker, Muhammad. (2021). Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities. IEEE Access. 9. 28177-28193. 10.1109/ACCESS.2021.3052867.
3. Banik, S., Chakraborti, A., Iwata, T., Minematsu, K., Nandi, M., Peyrin, T., Sasaki, Y., Sim, S. M., & Todo, Y. (2021). GIFT-COFB v1.1. Submission to the NIST LWC Standardization Process.((https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/gift-cofb-spec-final.pdf))
4. Catinca Mujdei, Lennert Wouters, Angshuman Karmakar, Arthur Beckers, Jose Maria Bermudo Mera, and Ingrid Verbauwhede. 2024. Side-channel Analysis of Lattice-based Post-quantum Cryptography: Exploiting Polynomial Multiplication. ACM Trans. Embed. Comput. Syst. 23, 2, Article 27 (March 2024), 23 pages. https://doi.org/10.1145/3569420.
5. Bhandari, J., Nabeel, M., Mankali, L., Sinanoglu, O., Karri, R., & Knechtel, J. (2024). Lightweight Countermeasures Against Static Power Side-Channel Attacks. *ArXiv*. https://arxiv.org/abs/2402.03196.
6. Bormann, C., Ersue, M., & Keranen, A. (2014). Terminology for Constrained-Node Networks (RFC 7228). Internet Engineering Task Force
7. Barenghi, Alessandro & Breveglieri, Luca & Koren, Israel & Naccache, David. (2012). Fault Injection Attacks on Cryptographic Devices. Proceedings of the IEEE. 100. 3056-3076. 10.1109/JPROC.2012.2188769.
8. W. J. Buchanan and L. Maglaras, "Review of the NIST Light-Weight Cryptography Finalists," 2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT), Pafos, Cyprus, 2023, pp. 469-474, doi: 10.1109/DCOSS-IoT58021.2023.00079.
9. Dinu, Daniel & Corre, Yann & Khovratovich, Dmitry & Perrin, Léo & Großschädl, Johann & Biryukov, Alex. (2019). Triathlon of lightweight block ciphers for the Internet of things. Journal of Cryptographic Engineering. 9. 10.1007/s13389-018-0193-x.
10. Dobraunig, C., Eichlseder, M., Mendel, F. et al. Ascon v1.2: Lightweight Authenticated Encryption and Hashing. J Cryptol 34, 33 (2021). https://doi.org/10.1007/s00145-021-09398-9
11. Islam, M. U., Nazish, M., Sultan, I., & Tariq Banday, M. (2024). ASCON Lightweight Security Standard for the Internet of Things Devices—A Study. In Proceedings of the International Conference on Innovative Computing and Communication (ICICC 2024) (Vol. 1024, pp. 503). Springer. https://doi.org/10.6028/NIST.SP.800-232
12. T. -H. Nguyen, D. -T. Dam, P. -P. Duong, B. Kieu-Do-Nguyen, C. -K. Pham and T. -T. Hoang, "Efficient Hardware Implementation of the Lightweight CRYSTALS-Kyber," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 72, no. 2, pp. 610-622, Feb. 2025, doi: 10.1109/TCSI.2024.3443238.
13. Weidong Lv, Yufei Chen, and Jia Liu "A survey of lightweight block cipher", Proc. SPIE 13403, International Conference on Algorithms, High Performance Computing, and Artificial Intelligence (AHPCAI 2024) , 134031T (18 November 2024); https://doi.org/10.1117/12.3051956
14. Madushan, H., Salam, I., & Alawatugoda, J. (2022). A Review of the NIST Lightweight Cryptography Finalists and Their Fault Analyses. Electronics, 11(24), 4199. https://doi.org/10.3390/electronics11244199
15. Malygina, E. & Kutsenko, Aleksandr & Novoselov, Semyon & Kolesnikov, N. & Bakharev, Aleksandr & Khilchuk, Irina & Shaporenko, A. & Tokareva, Natalia. (2024). Post-Quantum

Cryptosystems: Open Problems and Solutions. Lattice-Based Cryptosystems. Journal of Applied and Industrial Mathematics. 17. 767-790. 10.1134/S1990478923040087.
16. McGrew, David & Viega, John. (2004). The Security and Performance of the Galois/Counter Mode of Operation (Full Version). IACR Cryptology ePrint Archive. 2004. 193.
17. Mohajerani, Kamyar & Beckwith, Luke & Abdulgadir, Abubakr & Kaps, Jens-Peter & Gaj, Kris. (2025). Lightweight Champions of the World: Side-Channel Resistant Open Hardware for Finalists in the NIST Lightweight Cryptography Standardization Process. ACM Transactions on Embedded Computing Systems. 24. 1-25. 10.1145/3677320.
18. Nikova, Svetla & Rechberger, Christian & Rijmen, Vincent. (2006). Threshold Implementations Against Side-Channel Attacks and Glitches. 4307. 529-545. 10.1007/11935308_38.
19. Oswald, E., & Howe, J. (2021). Side Channels: Attacks, Defences, and Evaluation Schemes. NIST Crypto Club Presentation. Online: https://csrc.nist.gov/presentations/2021/side-channels-attacks-defences-and-evaluation-sche
20. Pereira, F.S., Correia, R., Pinho, P., Lopes, S.I., & Carvalho, N.B. (2020). Challenges in Resource-Constrained IoT Devices: Energy and Communication as Critical Success Factors for Future IoT Deployment. Sensors (Basel, Switzerland), 20.
21. Hasan and M. M. A. Hashem, "A Lightweight Cryptographic Framework Based on Hybrid Cellular Automata for IoT Applications," in IEEE Access, vol. 12, pp. 192672-192688, 2024, doi: 10.1109/ACCESS.2024.3519673.
22. Gușiță, B., Anton, A.A., Stângaciu, C.S. et al. Securing IoT edge: a survey on lightweight cryptography, anonymous routing and communication protocol enhancements. Int. J. Inf. Secur. 24, 149 (May 2025). https://doi.org/10.1007/s10207-025-01071-7
23. S. Sallam and B. D. Beheshti, "A Survey on Lightweight Cryptographic Algorithms," TENCON 2018 - 2018 IEEE Region 10 Conference, Jeju, Korea (South), 2018, pp. 1784-1789, doi: 10.1109/TENCON.2018.8650352
24. V. A. Thakor, M. A. Razzaque and M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," in IEEE Access, vol. 9, pp. 28177-28193, 2021, doi: 10.1109/ACCESS.2021.3052867.
25. Wouters, T. (March 2025). Hardware Implementation and Evaluation of the ROCKY Countermeasure for Ascon Against Fault Injection Attacks (Bachelor's thesis). Radboud University.