Computers, Materials & Continua

Tech Science Press

https://doi.org/10.32604/cmc.2026.087927

ARTICLE

Secure Communication in Wireless Sensor Networks Using Ascon Lightweight Cryptography

Kuldashbay Avazov[1], Jasur Sevinov[2,3], Komil Tashev[4], Jamila Arzieva[5], Tulkin Botirov[6], Alpamis Kutlimuratov[7], Akmalbek Abdusalomov[2,4,8,9,10,11], Boburjon Vafoev[12] and Young Im Cho[1,*]

[1]Department of Computer Engineering, Gachon University, Seongnam, Republic of Korea
[2]Department of Information Processing and Control Systems, Tashkent State Technical University, Tashkent, Uzbekistan
[3]Department of Computer Engineering, University of Tashkent for Applied Sciences, Tashkent, Uzbekistan
[4]Department of Computer Systems, Tashkent University of Information Technologies Named after Muhammad Al-Khwarizmi, Tashkent, Uzbekistan
[5]Department of Applied Mathematics and Computer Science, Karakalpak State University, Nukus, Uzbekistan
[6]Department of Automation and Control, Navoi State University of Mining and Technologies, Navoi, Uzbekistan
[7]Department of Applied Informatics, Kimyo International University in Tashkent, Tashkent, Uzbekistan
[8]Department of International Scientific Journals and Rankings, Alfraganus University, Tashkent, Uzbekistan
[9]Department of Digital Technologies and Mathematics, Kokand University, Kokand, Uzbekistan
[10]Department of Computer Engineering, Balıkesir University, Balıkesir, Türkiye
[11]Department of Software Engineering, Samarkand State University, Samarkand, Uzbekistan
[12]Department of Digital Economy, Tashkent State University of Economics, Tashkent, Uzbekistan

*Corresponding Author: Young Im Cho. Email: yicho@gachon.ac.kr

Received: 29 June 2026; Accepted: 17 August 2026; Published: 15 September 2026

ABSTRACT: Wireless sensor networks (WSNs) and Internet of Things (IoT) systems require lightweight cryptographic primitives that provide strong security under strict constraints on area, latency, and timing predictability. Ascon, selected by National Institute of Standards and Technology (NIST) as the standard for lightweight authenticated encryption, is well suited for such environments, yet application-oriented hardware implementations for WSN platforms remain underexplored. This paper presents a comprehensive evaluation of field programmable gate array (FPGA)-based Ascon architectures for secure WSN and IoT deployments, using iterative design with single permutation round and hybrid design with two-round unrolling across two FPGA classes. Implementations on Kintex UltraScale and Artix-7 devices achieve sub-microsecond deterministic latency, operating frequencies up to 273 MHz, and throughput (TP) between 300 and 620 Mbps, with resource usage as low as 1794 look-up tables (LUTs). A detailed hardware-to-hardware comparison with existing FPGA and application-specific integrated circuit (ASIC) implementations demonstrates the efficiency and design-space positioning of the proposed architectures. Application-level analysis, based on full multi-block cycle counts for 128-byte WSN-typical packets, shows support for hundreds of thousands of encrypted packets per second, exceeding the requirements of practical sensor-network workloads. The measured sub-microsecond latency and high TP demonstrate that the proposed architectures are well aligned with the performance and timing requirements of practical WSN and IoT deployments.

KEYWORDS: Ascon; authenticated encryption; FPGA; hardware acceleration; lightweight cryptography; WSN

1 Introduction

Wireless sensor networks (WSNs) have become a key enabling technology for numerous application domains, including environmental monitoring, industrial automation, smart agriculture, and critical infrastructure surveillance [1,2]. A typical WSN comprises numerous low-cost sensor nodes that sense, process, and transmit data wirelessly. However, these nodes have limited computational capability, memory, and communication bandwidth, making efficient and secure system design challenging.

WSNs face significant security risks due to their wireless medium, distributed architecture, and limited physical protection. Elsadig et al. [3] identify key threats, including eavesdropping, packet injection, and message modification, which compromise confidentiality and integrity. The SPINS (Security Protocols for Sensor Networks) framework [4] further emphasizes protection against replay attacks and node impersonation through authentication and data-freshness mechanisms. Boubiche et al. [5] classify these threats as passive (eavesdropping) and active (packet injection, replay, and impersonation) attacks and review corresponding countermeasures. Since WSNs may operate in unattended or hostile environments, confidentiality, integrity, authenticity, and freshness are essential.

Lightweight cryptography (LWC) addresses the security and resource constraints of embedded and low-power devices by providing efficient cryptographic protection with reduced computational and energy overhead. This is particularly important for WSNs, where conventional schemes such as the Advanced Encryption Standard (AES), although widely adopted and secure, can impose considerable computational overhead when implemented in software on low-power microcontrollers, increasing packet latency, energy consumption, and processor utilization [6–8]. To address these challenges, the National Institute of Standards and Technology (NIST) initiated the LWC standardization process for constrained environments, including WSNs and Internet of Things (IoT) devices [9]. Following extensive evaluation, Ascon was selected as the NIST standard for lightweight authenticated encryption with associated data (AEAD), providing confidentiality and integrity with improved suitability for resource-constrained platforms due to its security, simplicity, and efficiency across software and hardware implementations [10,11].

Although Ascon has been extensively analyzed and evaluated in software and hardware, its practical deployment in WSN nodes remains insufficiently explored. Existing studies largely focus on algorithm-level optimization or standalone hardware implementations, with limited consideration of system-level metrics such as packet latency, resource overhead, and real-time feasibility. This creates a gap in understanding how lightweight authenticated encryption (AE) can be integrated into WSN nodes while maintaining operational constraints.

Hardware-assisted cryptography offers a promising solution by offloading cryptographic operations to dedicated hardware, enabling low and deterministic latency, lower energy consumption, and improved separation of security and application logic [12]. Field programmable gate arrays (FPGAs) provide a flexible and reconfigurable platform for prototyping cryptographic accelerators and evaluating area, timing, throughput (TP), and power trade-offs before application-specific integrated circuit (ASIC) deployment [12,13]. However, limited research has examined the impact of FPGA-based lightweight AE on overall WSN performance and deployment feasibility.

FPGA and ASIC implementations of Ascon have increased rapidly, but most focus on optimizing the cryptographic core through round unrolling, pipelining, and resource sharing. Ahmet [12] achieved multi gigabit FPGA TP via aggressive round unrolling, while Khan et al. [13] introduced scalable iterative and partially unrolled FPGA designs delivering about 315 Mbps with 2060 look-up tables (LUTs) on a Spartan 6. Khan et al. [14] further demonstrated an ASIC design using configurable pipeline depths to enhance silicon efficiency. Although these studies report strong results in area, frequency, TP, and throughput per area

(TP/A), they largely evaluate Ascon as an isolated accelerator, offering limited insight into its suitability for real WSN deployments.

The motivation for this work is to provide strong security in WSNs without exceeding their computational, energy, and memory constraints. While Ascon is standardized for lightweight AE and several FPGA implementations exist, most studies emphasize hardware metrics rather than practical WSN requirements such as deterministic latency, energy efficiency, packet-processing capability, and deployment feasibility. This study therefore provides an application-oriented evaluation of representative FPGA-based Ascon architectures for secure, resource-constrained WSNs.

Two FPGA designs with different trade-offs are implemented on Kintex UltraScale and Artix-7 and assessed using both conventional hardware metrics and system-level measures. This integrated evaluation offers a clearer view of Ascon's practicality for WSN and IoT systems.

The main contributions of this paper are summarized as follows:

- Unlike previous Ascon hardware implementations that focused mainly on cryptographic performance, this work provides an application-oriented evaluation of FPGA-based Ascon by jointly analyzing hardware metrics and practical WSN deployment requirements.
- Two lightweight FPGA architectures based on iterative and hybrid two-round unrolled designs are implemented and evaluated on both Kintex UltraScale and Artix-7 FPGA platforms, demonstrating the trade-offs between area, TP, latency, power consumption, and energy efficiency.
- A comprehensive application-level evaluation is presented using deterministic latency, packet TP, and representative WSN packet sizes to demonstrate strong encryption can be achieved without compromising real-time communication requirements.
- Practical deployment considerations and design guidelines are provided to support architecture selection for different WSN and IoT devices.

The remainder of this paper is organized as follows. Section 2 reviews background and related work on WSN security and lightweight cryptographic implementations. Section 3 describes system architecture, while Section 4 presents proposed FPGA implementation of Ascon. Section 5 provides experimental results and discussion. Section 6 discusses the application-level evaluation, and Section 7 compares our work with existing approaches. Finally, Section 8 concludes the paper and outlines directions for future research.

2 Background and Related Work

2.1 Security in Wireless Sensor Networks: Software-Based Approaches and Limitations

Early WSN security research focused on software-based cryptographic protocols for constrained microcontrollers. SPINS and TinySec are representative examples, using symmetric-key cryptography to provide confidentiality, integrity, and data freshness [4,15]. Despite their practicality, software-based cryptographic implementations suffer from several limitations in modern WSN deployments. Implementing widely adopted cryptographic primitives, such as AES in software can incur substantial computational overhead, leading to increased packet latency. In addition to that, cryptographic computations executed on the main microcontroller compete with sensing, processing, and communication tasks, potentially degrading real-time performance. These limitations motivate the exploration of alternative approaches that can provide strong security guarantees without overwhelming the limited resources of sensor nodes.

2.2 Hardware Security for WSNs

Hardware-assisted security has emerged as a practical approach for offloading computationally intensive cryptographic operations from the main microcontroller to dedicated hardware accelerators. This separation reduces processor workload, enables deterministic execution, lowers cryptographic latency, and improves overall system efficiency compared with software-only implementations on resource-constrained platforms [13,16]. Dedicated hardware accelerators can execute cryptographic primitives more efficiently, offering predictable timing and reduced interference with sensing and networking tasks. However, few studies evaluate its impact on complete WSN operation, particularly packet latency, duty cycling, and overall node performance.

Recent literature on hardware realizations of lightweight cryptography, especially for resource-constrained IoT ecosystems, suggests that hardware implementations can adjust design choices (e.g., loop folding or unrolling) to trade off area and TP, but such studies tend to focus on synthesis metrics rather than application-level network performance [13]. This gap is significant because knowing how a hardware cryptographic block affects WSN operational constraints (latency, duty cycles, protocol timing) is critical to adopting these accelerators in real deployments, a topic that remains underexamined in current research.

Moreover, cryptographic security alone is insufficient for WSNs. Physically accessible sensor nodes require protection against implementation-level threats such as side-channel leakage, fault injection, and insecure nonce management. These considerations complement the underlying AE security and are important for secure hardware deployment.

2.3 Why Ascon is Suitable for WSNs

Ascon is a permutation-based AEAD algorithm selected by NIST as the final LWC standard, owing to its strong security guarantees, compact design, and efficiency on constrained platforms [11]. By combining encryption and authentication into a single primitive, Ascon reduces protocol complexity and communication overhead, which is particularly beneficial for WSNs where packet sizes and bandwidth are tightly constrained. Its simple Boolean operations, small internal state, and absence of complex arithmetic make Ascon well suited for both software and hardware implementations on low-power devices. Recent FPGA and ASIC studies further demonstrate that Ascon achieves favorable TP/A ratio efficiency compared to other lightweight ciphers, supporting flexible hardware design trade-offs for resource-constrained WSN nodes [14]. These properties make Ascon a practical and standardized choice for secure and energy-efficient communication in WSN deployments.

2.4 WSN Architecture, Constraints, and Threat Model

WSN nodes are typically composed of sensing elements, a low-power microcontroller, limited on-chip memory, and a short-range wireless transceiver. To maximize network lifetime, sensor nodes rely heavily on duty cycling and lightweight processing, making both computation and communication efficiency critical design considerations. Standards such as IEEE 802.15.4 further constrain packet size and timing, making large authentication tags or multi-stage cryptographic protocols impractical for many WSN deployments [7,16].

From a security perspective, WSNs are exposed to a wide range of passive and active attacks due to their wireless nature and frequent deployment in unattended or hostile environments. Adversaries may eavesdrop on traffic, inject forged packets, replay messages, or attempt impersonation to disrupt network operation or manipulate sensed data. In this work, the threat model assumes attackers with the capability to observe, modify, and inject wireless packets within communication range, but without physical access to

sensor nodes or the ability to compromise internal hardware cryptographic modules. Under this realistic threat model, lightweight AE is essential to ensure confidentiality, integrity, and authenticity while preserving energy efficiency and real-time performance in WSN applications [17].

2.5 Overview of Ascon and Related Hardware Implementations

Ascon is based on a sponge construction that relies on a compact permutation operating over a 320-bit internal state. Its design emphasizes simplicity and security, using only basic bitwise operations (AND gate, XOR gate, rotations) and avoiding complex arithmetic, which makes it inherently well-suited for constrained hardware platforms.

Its core component, the permutation, operates on a 320-bit state and consists of multiple rounds combining a nonlinear substitution layer based on 5-bit S-boxes with linear diffusion achieved through bitwise rotations and XOR operations. The internal architecture for one round of permutation function is provided in Fig. 1. The number of rounds is parameterized to balance security and performance, with different variants using distinct round counts for initialization, associated data (AD) and plaintext/ciphertext processing, and finalization.

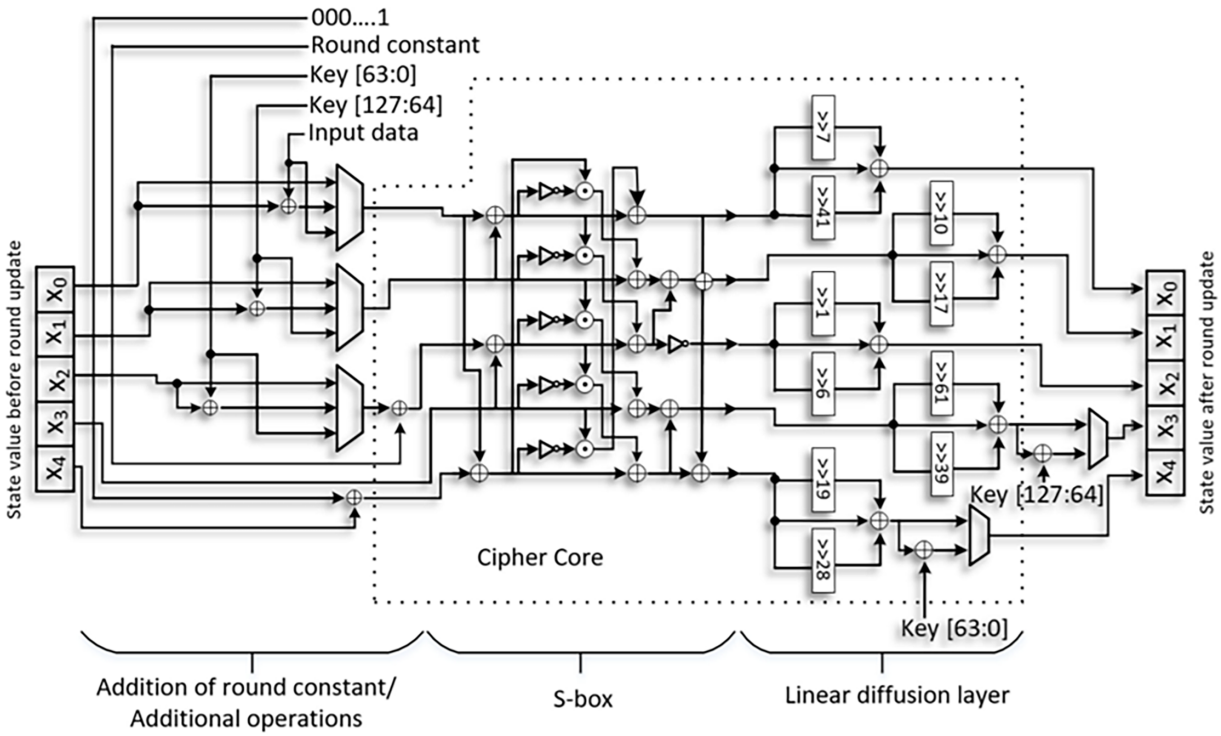

Figure 1: One round of the permutation function [13].

Although previous studies significantly advance the hardware implementation of Ascon, they primarily evaluate implementation metrics. Limited attention has been given to application-level evaluation, including packet-processing capability, deterministic latency, deployment feasibility, and the practical requirements of wireless sensor networks. Table 1 summarizes comparison with previous works.

Our work extends this body of research by embedding a hardware-accelerated Ascon implementation within WSN node architecture and analyzing its impact on critical system metrics. By doing so, we

provide insights into how Ascon's hardware advantages translate into practical improvements in network responsiveness, energy efficiency, and security for wireless sensor deployments.

Table 1: Comparison with previous works.

Feature	[12]	[13]	[14]	This Work
FPGA implementation	✓	✓	✗	✓
ASIC implementation	✗	✗	✓	✗
Iterative architecture	✗	✓	✓	✓
Partially unrolled architecture	✓	✓	✓	✓
Multi-platform evaluation	✗	✗	✗	✓
WSN-specific evaluation	✗	Limited	✗	✓
Packet-level TP analysis	✗	✗	✗	✓
Deterministic latency analysis	Limited	Limited	✗	✓
Energy per encryption	✗	✗	✗	✓

3 System Architecture

Fig. 2 illustrates the proposed architecture of a secure WSN node employing a hardware-accelerated lightweight cryptographic scheme. The architecture comprises three main components: a general-purpose microcontroller unit (MCU), an FPGA-based cryptographic accelerator, and a wireless radio module. While our work focuses on the FPGA implementation of Ascon, the overall design considers practical WSN deployments where these components interact to provide secure data transmission.

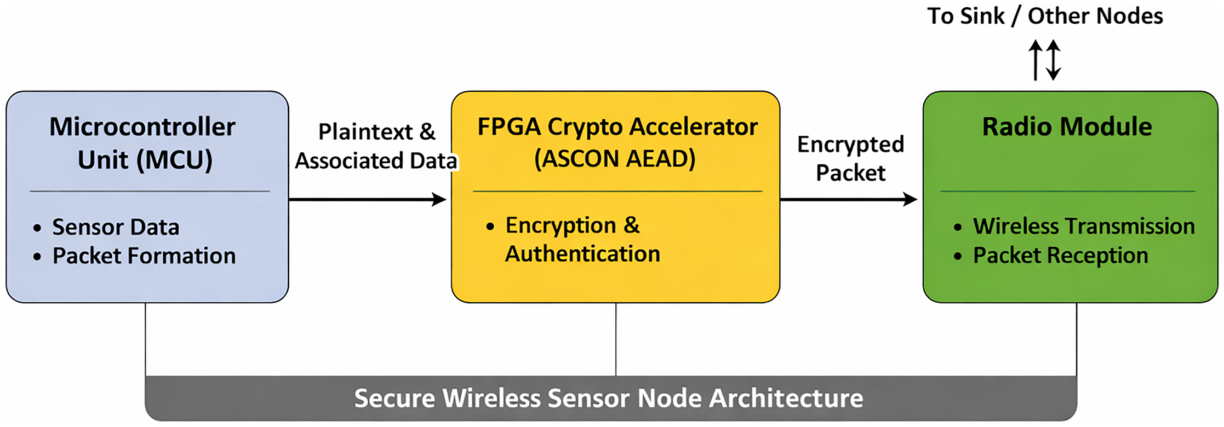

Figure 2: System architecture.

- Microcontroller Unit (MCU): The MCU manages sensor interfacing, data acquisition, packet formation, and network protocol operations. It also coordinates data transfer between the sensor, cryptographic accelerator, and radio module.
- FPGA Crypto Accelerator: The FPGA operates as a dedicated cryptographic co-processor, offloading Ascon-based AEAD operations from the MCU. It performs payload encryption and authentication-tag generation in hardware, thereby reducing software processing overhead and cryptographic latency.

- Radio Module: The radio module provides wireless communication with neighboring nodes or sink devices. After cryptographic processing, the MCU forwards the authenticated ciphertext and associates protocol information to the radio for transmission.

During operation, the MCU collects sensor data, prepares the packet and AD, and forwards them to the FPGA accelerator. The FPGA executes the Ascon AEAD operation to encrypt the payload and generate the authentication tag. The MCU then receives the resulting ciphertext and tag, adds the required protocol headers, and forwards the secured packet to the radio module for uplink, downlink, or peer-to-peer transmission.

By performing cryptographic operations in dedicated hardware, the proposed architecture reduces MCU computational overhead and latency while providing confidentiality and integrity protection. This hardware–software partitioning is particularly suitable for resource-constrained WSN nodes, where energy efficiency and computational performance are critical. The following sections present the FPGA implementation of Ascon and evaluate its performance in terms of area, latency, and power consumption.

4 FPGA Based Implementation of Ascon

In this section, we present the hardware design and FPGA implementation of the Ascon algorithm. The core primitive of Ascon is a permutation function, denoted by p, which operates on a 320-bit internal state. The permutation consists of multiple rounds, and each round comprises three main steps: addition of round constants, a non-linear substitution layer implemented using a 5-bit S-box applied in a bit sliced manner, and a linear diffusion layer based on rotations and XOR operations. For Ascon-128, two instances of permutation are employed: the full permutation p^{12}, which consists of 12 rounds, and the reduced permutation p^6, which consists of 6 rounds.

As shown in Fig. 3, Ascon algorithm operates in four phases: initialization, AD processing, plaintext processing, and finalization. During initialization, the internal state is constructed from the initialization vector IV, the secret key K, and the nonce N, followed by the application of the full permutation p^{12}. AD blocks are absorbed into the state by XORing them into the rate part, with each block followed by reduced permutation p^6 and appropriate domain separation. Plaintext encryption (or ciphertext decryption) is performed by XORing plaintext blocks with the rate portion of the state to generate ciphertext blocks, again followed by p^6 for each processed block. In the finalization phase, the key K is reintroduced into the state, the full permutation p^{12} is applied, and the authentication tag T is extracted. The 320-bit state is organized into five 64-bit words x_0, x_1, x_2, x_3, and x_4, where x_0 constitutes the rate, while x_1 to x_4 form the capacity, including the key-dependent components of the state.

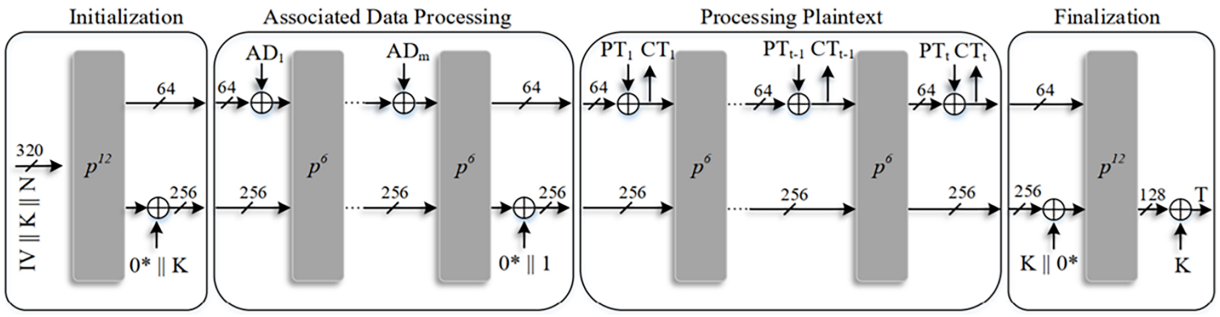

Figure 3: Overall architecture of Ascon [13].

Given the resource constraints of WSNs, where low area is critical, we propose two distinct hardware architectures for Ascon on FPGA. These architectures balance TP, area efficiency, and latency. The first is baseline architecture, a fully unrolled combinational design for high TP. The second is a round-iterative design that reuses a single permutation round module to minimize area. The third is a hybrid design that unrolls two rounds per clock cycle, offering a trade-off between the first two. All architectures are implemented in Verilog hardware description language (HDL) and targeted for Kintex UltraScale and Xilinx Artix-7 FPGA, with synthesis using Vivado.

4.1 Architecture 1: Fully Unrolled Combinational Design

This architecture serves as baseline and directly maps the entire Ascon data path into a combinational circuit, unrolling all permutation rounds without sequential logic between rounds. It prioritizes maximum TP at the cost of higher area utilization, making it suitable for applications where speed is paramount and area is less constrained.

The top-level module includes inputs for the 128-bit key K, 128-bit nonce N, AD (padded to 64-bit blocks), plaintext (padded to 64-bit blocks). Outputs include ciphertext and authentication tag.

The state register is 320 bits, initialized as follows: $x_0 = IV$ (initialization vector, 0x80400c0600000000 for Ascon-128), $x_1 \parallel x_2 = K$, $x_3 \parallel x_4 = N$. The initialization phase applies the full 12-round permutation p^a in a single combinational path. Each round is implemented as a cascade of sub-modules:

Constant Addition: XORs a round-specific constant (e.g., 0xf0 for round 0) into x_2. Substitution: Applies a 5-bit S-box to each of the 64 slices of the state in parallel. The S-box is implemented using LUTs for efficiency. Linear Diffusion: In the fully unrolled hardware architecture, the linear diffusion layer of the Ascon permutation is implemented purely using combinational XOR and fixed rotation operations, eliminating control overhead and enabling maximum TP at the cost of increased area.

Since all 12 rounds for p^a (and 6 for p^b) are unrolled, the data path forms a deep combinational logic chain. For AD processing, each 64-bit block is XORed into x_0, followed by p^b. Similarly, for message blocks, plaintext is XORed into x_0 to produce ciphertext, with p^b applied afterward. Finalization extracts $x_3 \parallel x_4$ as the tag after another p^a. On FPGA, this design consumes significant resources due to the replication of S-boxes (64 per round × 12 rounds = 768 S-boxes) and rotation logic, however, this can be the highest TP design.

4.2 Architecture 2: Round-Iterative Design with Single Permutation Round

To optimize for area, especially in resource-constrained WSNs, this architecture reuses a single permutation round module iteratively across all rounds of Ascon. This serialized approach trades TP for reduced hardware footprint, ideal for low-power devices where operations can be spread over multiple clock cycles. The design features a 320-bit state register, a round counter, and a finite state machine (FSM) controlling the phases: idle, initialization, AD processing, message processing, finalization, and done. The core is a single-round permutation module, which takes the current state as input and outputs the next state after one round's operations. The architecture is depicted in Fig. 4.

The permutation round module is implemented as combinational logic, including a multiplexer for selecting the round constant, 64 parallel 5-bit S-boxes for p_S, and barrel shifters for linear diffusion layers, using FPGA's fast carry chains for XOR operations. The FSM iterates this round module for exactly 12 clock cycles during the initialization and finalization phases where p^a is applied, and for 6 clock cycles during each AD or message block processing where p^b is used. The internal state during the permutation is held in the 320-bit state registers. For multi-block inputs, the number of iterations scales with the number of blocks, with each block requiring 6 cycles for p^b plus additional cycles for data injection and XOR operations.

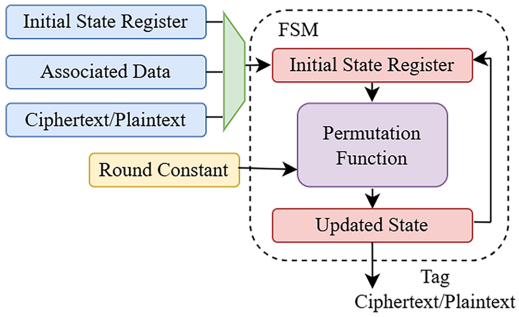

Figure 4: Round-iterative design with single permutation round.

Between phases, inputs are XORed into the state: for example, AD blocks are XORed into x_0, followed by the iterative application of the round module; similarly, message blocks are XORed for encryption or decryption. This architecture significantly reduces area by instantiating only 64 S-boxes and one set of diffusion logic, which are re-used temporally across cycles. On FPGA, it uses fewer LUTs compared to the unrolled design but requires more clock cycles overall (e.g., 12 cycles for each p^a, 6 cycles per p^b, plus overhead for data handling and phase transitions). TP is accordingly lower, making it suitable for WSNs with intermittent data transmission where high speed is not critical. The critical path is shorter, limited to one round's combinational delay, allowing higher clock frequencies.

4.3 Architecture 3: Hybrid Design with Two-Round Unrolling

This architecture provides a balance between the high-TP unrolled design and the area-efficient iterative one by unrolling two permutation rounds per clock cycle. It processes two rounds in each cycle, effectively halving the latency compared to the single-round iterative design while saving area relative to full unrolling. This hybrid approach is particularly advantageous for WSNs, where moderate TP is required without excessive resource utilization. Like Architecture 2, it includes a 320-bit state register, a round counter, and an FSM managing the operational phases. However, the core permutation module now cascades two full rounds in a single combinational logic path: the first round followed directly by the second round. The architecture is depicted in Fig. 5.

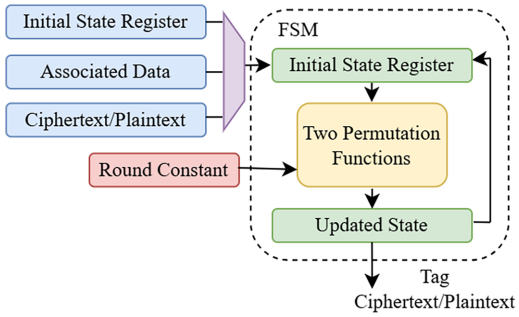

Figure 5: Hybrid design with two-round unrolling.

The two-round permutation module features combinational logic with two sets of round constant multiplexers (selected pairwise, e.g., for rounds 0 and 1), two banks of 64 S-boxes (one for each round), and sequential diffusion layers for each round. The FSM iterates this module for p^a in 6 clock cycles (since 12 rounds are covered two at a time) and for p^b in 3 clock cycles (6 rounds similarly paired). For each AD or message block, this results in 3 cycles per p^b, with data injection (e.g., XOR of AD or message

into x_0) occurring between iterations. Initialization and finalization each take 6 cycles for their respective p^a applications.

Area-wise, this design requires slightly more resources than Architecture 2, (128 S-boxes and two sets of diffusion logic instead of one), but it remains far more compact than the fully unrolled Architecture 1. TP is effectively increased compared to the iterative de-sign, with overall latency reduced (e.g., 6 cycles per p^a instead of 12), enabling faster processing of multi-block messages in WSN scenarios. The critical path is longer than that of a single round but still manageable.

The proposed FPGA architectures for Ascon were designed to address different priorities in resource-constrained WSNs: the fully unrolled combinational design maximizes TP and minimizes latency by processing all permutation rounds in a single clock cycle through a deep logic path, at the cost of high area usage; the round-iterative design with a single permutation round drastically reduces area and power by reusing the same hardware over 12 or 6 clock cycles per phase, accepting lower TP for ultra-low-resource nodes; while the hybrid two-round unrolling design offers a balanced compromise by processing two rounds per cycle (halving the latency of the iterative approach while using only moderately more area), making it well-suited for mid-tier WSN applications that need reasonable speed without excessive resource consumption.

The architectures presented in this work focus on functional correctness and performance and do not incorporate side-channel countermeasures such as masking or hiding. We also assume that key storage, key provisioning, and nonce-uniqueness enforcement are handled securely by the MCU or a trusted system component. As such, the proposed designs should be viewed as application-oriented accelerators rather than complete secure implementations, and additional protections would be required for deployment in adversarial physical environments.

5 Experimental Results and Discussion

This section presents and analyzes the post-synthesis and post-implementation results of the proposed Ascon hardware architectures on two different FPGA platforms: the high-performance Kintex UltraScale XCKU035-FFVA1156-3-E and the cost-sensitive, automotive-grade Artix-7 XA7S100FGGA676-1Q. The evaluation focuses on Architecture 2 (single-round iterative) and Architecture 3 (two-round hybrid unrolled) for the encryption operation of Ascon-128. All designs were implemented using the Xilinx Vivado Design Suite.

The following metrics are reported in Tables 2 and 3:

- **Area**: Number of LUTs, serving as the primary area metric on FPGAs.
- **Latency (Lat.)**: Number of clock cycles required to complete one AE operation.
- **Maximum Frequency (FMAX)**: Achievable clock frequency after place-and-route.
- **Encryption Time**: Total time required to complete one encryption operation, calculated as Latency/FMAX.
- **Throughput (TP)**: Computed as Block Size × FMAX/Latency.
- **Throughput per Area (TP/A)**: Efficiency metric expressed as Mbps per LUT.

Table 2: Implementation results on Kintex UltraScale XCKU035-FFVA1156-3-E.

Architecture	Area (LUTs)	Lat. (cc)	F_{MAX} (MHz)	Time (ns)	TP (Mbps)	TP/A (Mbps/LUT)	P (mW)	E/Enc (nJ)
Architecture 2	1794	42	273.03	153.83	416.05	0.231	45	6.95
Architecture 3	2472	24	232.61	103.17	620.29	0.250	97	10.01

Table 3: Implementation results on Artix-7 XA7S100FGGA676-1Q.

Architecture	Area (LUTs)	Lat. (cc)	F_{MAX} (MHz)	Time (ns)	TP (Mbps)	TP/A (Mbps/LUT)	P (mW)	E/Enc (nJ)
Architecture 2	2045	42	196.96	213.24	300.12	0.146	37	7.89
Architecture 3	2902	24	137.91	174.02	367.76	0.126	68	11.83

For Architecture 1, the area consumption in terms of LUTs is around 14.4k with a TP of 766 Mbps. This corresponds to the baseline implementations of Ascon where the area utilization is maximum.

For architecture 2 and 3, on the high-performance Kintex UltraScale platform, both architectures achieve high operating frequencies due to the advanced 20 nm UltraScale fabric and improved routing resources. Architecture 2 reaches a peak frequency of 273.03 MHz, taking advantage from its short critical path derived from executing a single Ascon permutation round per cycle. Architecture 3, despite increasing the amount of combinational logic per cycle, still achieves 232.61 MHz, corresponding to only a 14.5% reduction in frequency. This demonstrates that the two-round unrolled data path scales efficiently on modern FPGA architectures with fast carry chains and optimized interconnect.

The key advantage of Architecture 3 on this platform is its significantly reduced latency (24 cycles compared to 42 cycles), which directly translates into a substantial TP improvement. Architecture 3 achieves 620.29 Mbps, representing a 49.7% increase over Architecture 2. Importantly, this TP gain is not achieved at the expense of efficiency: the TP/A metric slightly improves from 0.231 to 0.250 Mbps/LUT. This confirms that, on UltraScale devices, the hybrid two-round unrolling strategy provides a highly favorable trade-off between area and performance.

In contrast, the behavior on the Artix-7 XA7S100 device highlights the impact of technology scaling and routing constraints. While Architecture 2 maintains a reasonable operating frequency of nearly 197 MHz, Architecture 3 experiences a pronounced frequency degradation to 137.9 MHz (approximately 30% lower). This larger penalty is attributed to the longer critical path introduced by the two-round combinational cascade and the comparatively limited routing and timing optimization capabilities of the 28 nm Artix-7 fabric.

As a result, the TP advantage of Architecture 3 on Artix-7 is reduced to 22.5% (367.76 vs. 300.12 Mbps). More importantly, the TP/A metric reverses in favor of Architecture 2, with TP/A values of 0.146 and 0.126 Mbps/LUT, respectively. This reversal clearly indicates diminishing returns from partial unrolling on lower-end devices, where additional logic increases routing congestion and limits achievable frequency.

To improve the reproducibility of the application-level performance analysis, the packet encryption latency is derived from the execution phases of the Ascon AE algorithm. For each packet, the total encryption latency is expressed as

$$T_{total} = T_{init} + T_{AD} + N_{msg} \times T_{perm} + T_{final},$$

where T_{init} denotes the initialization phase, T_{AD} represents AD processing, N_{msg} is the number of 128-bit message blocks, T_{perm} is the execution time of one permutation, and T_{final} includes the finalization phase and authentication-tag generation.

The analysis considers only the FPGA accelerator execution time. MCU–FPGA communication, bus-transfer, protocol, radio, and software overheads are excluded as they depend on the target platform and interface. Thus, the reported packet TP reflects the cryptographic accelerator performance for representative WSN packet sizes.

In addition to area, latency, and TP, we extend our evaluation with power and energy analysis to better reflect the requirements of resource-constrained WSN and IoT systems. Power estimation was performed using post-implementation analysis in Xilinx Vivado Design Suite, incorporating switching activity from timing simulation.

On the Kintex UltraScale platform, Architecture 2 and Architecture 3 exhibit power consumption of 45 and 97 mW, respectively. The higher power observed in Architecture 3 is primarily due to the increased combinational logic and switching activity introduced by two-round unrolling.

To provide a more application-relevant metric, we compute energy per encryption operation using the measured latency values. Architecture 2 achieves an energy consumption of approximately 6.95 nJ per encryption, whereas Architecture 3 requires approximately 10.01 nJ. These results indicate that the iterative architecture is more energy-efficient, while the hybrid architecture prioritizes performance via higher TP.

For completeness, we also consider the Artix-7 platform. The power consumption is 37 mW for Architecture 2 and 68 mW for Architecture 3. Using the corresponding latency values, the energy per encryption is approximately 7.89 and 11.83 nJ, respectively. Despite the lower absolute power on Artix-7, the same trend is observed across both FPGA families: Architecture 2 provides better energy efficiency, while Architecture 3 offers higher TP. These results highlight a clear and consistent design trade-off between energy efficiency and performance, enabling system designers to select appropriate architecture based on application-specific constraints.

These results highlight a strong device-dependent design trade-off. Architecture 3 is best suited for modern, high-performance FPGA families where aggressive unrolling can be exploited to maximize TP with minimal efficiency loss. Conversely, Architecture 2 emerges as a more balanced and cost-effective solution for older or resource-constrained devices, particularly relevant for WSN deployments where silicon cost, timing margin, and robustness are prioritized over peak TP.

Table 4 summarizes representative FPGA implementations of Ascon from [12,13], providing a useful baseline for understanding the broader hardware design space. The high TP architectures in [12] achieve multi-gigabit performance by aggressively unrolling the permutation rounds, but this comes at the cost of large combinational data paths, higher LUT utilization, and long critical paths. Such designs are well suited to performance-oriented FPGA platforms but are not appropriate for resource-constrained WSN nodes, where area, energy per packet, and predictable timing behavior are more critical than peak TP. The iterative Spartan-6 design in [13] reduces area but delivers significantly lower TP and efficiency, and it does not target any specific WSN system model. It is also important to note that the implementation in [14] is an ASIC design, although it provides valuable insight into area–TP trade-offs in silicon, it is not directly comparable to FPGA-based results due to fundamental differences in technology, optimization flow, and performance scaling.

Table 4: Comparison with existing FPGA architectures.

Reference	Platform	Area. (LUTs)	F_{MAX} (MHz)	TP (Mbps)	TP/A	Primary Focus
[12]	Kintex-7	2958	92.59	5925.9	2.01	Maximum TP through aggressive round unrolling
[12]	Artix-7	2957	55.25	3535.9	1.19	High-performance FPGA implementation
[13]	Spartan-6	2060	206.26	315.2	0.15	Area-efficient iterative FPGA implementation

(Continued)

Table 4 (continued)

Reference	Platform	Area. (LUTs)	F_{MAX} (MHz)	TP (Mbps)	TP/A	Primary Focus
[14]	ASIC	–	–	–	–	ASIC implementation targeting silicon efficiency
Ours	Kintex	1794	273.03	416.0	0.231	WSN-oriented iterative architecture
Ours	Kintex	2472	232.61	620.3	0.250	WSN-oriented hybrid architecture

In contrast, our work is explicitly designed for the operational characteristics of WSN devices. Rather than maximizing raw TP, our architectures are evaluated using realistic WSN considerations that reflect how a sensor node processes data. This leads to architectural choices that balance area, latency, and TP in a way that neither [12,13], nor the ASIC-oriented work in [14] address. As a result, although prior designs may achieve higher absolute TP on general-purpose FPGAs or ASICs, our application-oriented evaluation focuses on their practical suitability for resource-constrained and battery-powered WSN devices.

The flexibility in implementation enables system designers to select the most appropriate Ascon hardware architecture based on target FPGA family and application-specific TP vs. area requirements, making the designs highly suitable for secure and resource-constrained WSN and IoT environments.

MCU–FPGA data-transfer overhead is not included in the current analysis because it depends on the communication interface (e.g., Serial Peripheral Interface (SPI), Advanced eXtensible Interface (AXI), Universal Asynchronous Receiver/Transmitter (UART), or memory-mapped bus) and the target hardware platform. Quantifying this overhead requires a complete embedded prototype, which is beyond the scope of the present work and will be investigated in future work.

6 Application-Level Evaluation

While raw TP and area efficiency are important metrics for cryptographic accelerators, their practical relevance is best understood when mapped to real application requirements. This section evaluates the proposed Ascon FPGA architecture at the application level, focusing on representative WSN and IoT scenarios.

WSN and IoT nodes typically transmit small to medium-sized packets (e.g., 64–128 bytes for environmental monitoring, industrial sensing, or control data) at relatively low data rates, often in the range of 50–250 kbps for protocols such as Zigbee or IEEE 802.15.4. These systems impose stringent requirements on low latency and secure AE, where cryptographic overhead must remain negligible compared to wireless transmission time. Typical application scenarios include periodic sensor reporting (e.g., temperature or humidity updates every few seconds), event-driven alerts, and aggregated data forwarding to a gateway or cluster head.

6.1 Encrypted Packet Throughput in WSN and IoT Gateways

Using the measured TP values from the experimental results, we estimate the number of encrypted packets supported per second, assuming a conservative packet size of 128 bytes. This packet size reflects a typical Ascon-128 AEAD configuration, including payload, AD, and authentication tag, and accounts for the full encryption process (initialization, processing, and finalization).

On the Kintex UltraScale XCKU035 platform, Architecture 2 achieves a TP of 416.05 Mbps, corresponding to approximately 406,000 encrypted 128-byte packets per second. Architecture 3 further increases this capability to approximately 606,000 packets per second at 620.29 Mbps. These rates significantly exceed the demands of common WSN gateway scenarios. For example, in a dense deployment with 100 sensor nodes transmitting one 128-byte packet per second, the aggregate data rate is approximately 0.1024 Mbps (102.4 Kbps). Architecture 3 therefore provides approximately 6057× TP headroom, enabling secure handling of bursty traffic, multi-sensor fusion, or gateway-level aggregation without introducing TP bottlenecks.

On the cost-sensitive Artix-7 platform, Architecture 2 supports approximately 293,000 encrypted packets per second, while Architecture 3 supports around 359,000 packets per second. Despite the lower operating frequency of this device family, both architectures remain well suited for edge gateways and embedded aggregation points in industrial WSNs, smart agriculture, and environmental monitoring systems, where individual nodes typically generate only 1–10 packets per second.

The packet rate figures reported above are derived from the full multi block execution time required to process a 128-byte message, rather than from the minimum single block latency values listed in Tables 2 and 3. The single block results are provided for architectural comparison with prior hardware designs, whereas the packet level analysis presented here uses the complete cycle count for all permutation blocks involved in a 128-byte packet.

6.2 Latency Analysis for Time-Critical Applications

Latency is a critical metric for real-time and safety-related embedded systems. The measured encryption latencies are extremely low: on the Kintex UltraScale device, Architecture 2 completes an Ascon encryption operation in 153.83 ns, while Architecture3 requires only 103.17 ns. On the Artix-7 device, the corresponding latencies are 213.24 and 174.02 ns, respectively.

These sub-microsecond encryption delays are well below the latency requirements reported for many industrial applications. For example, industrial safety applications may require deterministic latency of up to 10 ms, while closed-loop control applications typically require 10–100 ms and monitoring applications may tolerate around 100 ms [18]. Recent IIoT requirements similarly report end-to-end latency targets ranging from 1 to 100 ms for real-time industrial applications [19]. Compared with these application-level requirements, the proposed hardware accelerators introduce negligible cryptographic processing delays. Therefore, the results indicate that AE can be integrated without becoming a significant contributor to the overall timing budget of latency-sensitive WSN and IIoT applications.

The reported latency represents the hardware permutation core in isolation. In practical WSN deployments, MCU–FPGA data-transfer and wireless delays may dominate overall execution time. Nevertheless, with communication delays typically in the millisecond range, the sub-microsecond cryptographic latency remains negligible in the overall timing budget.

6.3 Architecture Selection for WSN and IoT Deployments

The application-level evaluation highlights a clear deployment-oriented trade-off between the proposed architectures. Architecture 3 is particularly well suited for high-performance roles such as IoT gateways or cluster heads in dense WSN deployments. Its higher TP and lower per-packet latency enable a single accelerator instance to service a large number of nodes or high-rate aggregated traffic streams efficiently.

In contrast, Architecture 2 provides a highly attractive solution for cost-constrained deployments, especially on 7-series devices such as Artix-7. Its smaller area footprint, shorter critical path, and favorable

TP/A characteristics make it easier to integrate alongside networking stacks, control logic, and system-level management functions, while still delivering performance far more than typical WSN node requirements.

Overall, the results confirm that both proposed Ascon architectures comfortably meet the TP and latency demands of practical WSN and IoT applications. By offloading AE to dedicated hardware with negligible overhead, the designs enable secure and real-time communication in resource-constrained environments.

The application-level results presented in this section are derived from analytical mapping of measured FPGA performance to typical WSN packet sizes and timing constraints. Although a full protocol-stack implementation is beyond the scope of this work, the deterministic sub-microsecond latency and high packet-level TP demonstrate that hardware-accelerated Ascon is technically feasible for real-time WSN communication.

7 Comparison with Existing WSN Security Approaches and Deployment Considerations

This section positions the proposed Ascon hardware architectures within the broader security landscape of WSNs by comparing them with widely used software-based schemes, including AES-128 and lightweight ciphers such as PRESENT. Although hardware accelerators for these algorithms exist, software implementations on resource-constrained MCUs remain common due to their flexibility and low hardware cost. The comparison focuses on key WSN considerations, including latency, resource utilization, scalability, and deployment practicality.

7.1 Comparison with Software-Based WSN Security Implementations

Latency and Timing Predictability:

Software implementations of cryptographic primitives such as AES and lightweight block ciphers exhibit significant execution-time variability due to interrupts, task scheduling, shared memory buses, and power-management events in embedded operating systems [8,20]. For a typical 128-byte WSN packet (including AD and authentication tag), software AES-128-CCM (Counter with Cipher Block Chaining Message Authentication Code) commonly requires significant CPU cycles on low-end MCUs, resulting in end-to-end encryption latency that can be high in resource-constrained contexts. Lightweight ciphers such as PRESENT reduce code size but frequently incur comparable or higher latency (5–20 ms for full AE), owing to bit-serial processing and limited instruction-level parallelism on low-end MCUs [21]. This variability introduces timing jitter, complicating worst-case execution time (WCET) analysis in real-time and safety-critical WSN deployments.

In contrast, the proposed Ascon hardware architectures provide fully deterministic execution with fixed and predictable cycle counts. FPGA-based Ascon implementations report sub-microsecond critical-path latency and tightly bounded encryption latency independent of system load or traffic patterns [13]. Such determinism is essential for time-sensitive WSN applications, where missed deadlines can compromise system reliability [22].

The software latency comparison for AES-128-CCM and PRESENT are included solely to provide high-level context on the typical performance limitations of software-only AEAD schemes on constrained MCUs. These are not used to claim quantitative speedup.

Resource Contention:

In software-centric WSN nodes, cryptographic processing competes directly with sensing tasks, protocol stacks, and application logic for CPU cycles and memory bandwidth [17]. Empirical studies show that software-based encryption can consume 20%–50% of MCU processing time per packet in constrained IoT

platforms, particularly when combined with communication and sensing workloads [23]. This contention becomes especially problematic under bursty traffic conditions or multi-sensor data aggregation scenarios.

The proposed Ascon hardware architectures eliminate this contention by offloading AE entirely to dedicated logic. On Artix-7-class FPGA platforms, Architecture 2 requires approximately 2045 LUTs while maintaining high operating frequency, whereas Architecture 3 increases area to around 2902 LUTs but significantly improves TP. Compared with reported hardware implementations of AES or PRESENT, which typically require 3000–6000 LUTs on comparable FPGA families with lower TP/A efficiency [24], the proposed designs achieve competitive efficiency of 0.126–0.146 Mbps/LUT on Artix-7, making them well suited for resource-constrained WSN nodes and edge gateways.

The comparison with software-based AES and PRESENT uses representative latency and resource figures from WSN literature rather than measurements on an identical platform. Thus, the results provide an indicative, order-of-magnitude comparison. While the proposed Ascon designs use measured FPGA latency and TP mapped to typical WSN packet sizes, AES/PRESENT values reflect MCU-based software execution. The comparison therefore highlights relative trends, such as deterministic hardware timing and reduced MCU contention, rather than a platform-equivalent benchmark.

It should be noted that the comparisons include implementations using different FPGA families, technology nodes, synthesis tools, and optimization objectives. Therefore, the reported metrics should be regarded as indicative rather than direct one-to-one benchmarks, as implementation environments can affect resource utilization, frequency, TP, and power consumption.

7.2 Scalability and Key Management Considerations

From a scalability perspective, the high TP achieved by the proposed architecture enables a single hardware instance to serve large numbers of sensor nodes or multiple concurrent communication channels. Architecture 3 is particularly suitable for gateways and cluster heads aggregating traffic from dense deployments, while Architecture 2 provides an area- and energy-efficient solution for cost- and power-constrained edge nodes.

Key management is treated at a high level in this work and follows established WSN practice. The architecture assumes external provisioning of keys and nonces via pre-shared keys or lightweight key-establishment protocols such as Datagram Transport Layer Security (DTLS) or Ephemeral Diffie-Hellman Over COSE (EDHOC) [25]. Ascon's 128-bit security level, standardized by NIST for lightweight cryptography, provides strong resistance against classical attacks and improved robustness against quantum adversaries (e.g., Grover's algorithm) compared to ultra-lightweight ciphers such as PRESENT, while avoiding several implementation complexities associated with AES.

7.3 Limitations and Deployment Considerations

Despite their advantages, the proposed designs have limitations that must be considered in deployment. While Ascon is well suited for hardware implementation, protection against side-channel attacks, such as power or electromagnetic analysis, requires additional countermeasures. Threshold- or masking-based implementations can introduce significant hardware overhead; for example, a threshold implementation of Ascon has been reported to require approximately 3.1× the area of an unprotected low-area implementation [26]. Such protected implementations are beyond the scope of this work but represent an important direction for future research.

Overall, compared to traditional software-based AES or PRESENT implementations commonly used in WSNs, the proposed Ascon hardware architectures deliver orders-of-magnitude lower latency, fully

deterministic timing behavior, and elimination of computational contention. These properties make them particularly attractive for real-time, industrial, automotive, and gateway-centric IoT deployments. When integrated with existing protocol stacks such as IEEE 802.15.4, Message Queuing Telemetry Transport (MQTT), Long Range Wide Area Network (LoRaWAN), or Controller Area Network with Flexible Data-Rate (CAN-FD)-inspired networks, the proposed designs enable scalable and secure communication without compromising the low-power and real-time requirements of modern WSNs.

Practical deployment also requires complementary safeguards, including secure key storage, robust nonce management, and tamper protection. Combined with future side-channel-resistant designs, these measures are essential for end-to-end security in real-world WSNs. The proposed methodology therefore extends beyond TP optimization by considering deterministic latency, encrypted-packet TP, and WSN/IoT deployment feasibility alongside hardware metrics, enabling architecture selection based on performance, area, and energy constraints.

8 Conclusion

This paper presented and evaluated two FPGA-based hardware architectures for implementing the lightweight AE algorithm Ascon in WSN applications. The proposed iterative architecture (Architecture 2) and hybrid two-round unrolled architecture (Architecture 3) were implemented and evaluated on both Kintex UltraScale and Artix-7 FPGA platforms to investigate the trade-offs between hardware resource utilization, TP, latency, power consumption, and energy efficiency.

The experimental results demonstrate that Architecture 2 provides a highly area-efficient implementation, requiring only 1794 LUTs on the Kintex UltraScale FPGA while achieving a TP of approximately 416.0 Mbps with a power consumption of 45 mW and an energy consumption of 6.95 nJ per encryption. In comparison, Architecture 3 increases hardware utilization to 2472 LUTs, but improves TP to approximately 620.3 Mbps, representing an increase of nearly 50%, at the expense of higher power consumption (97 mW) and energy consumption (10.01 nJ per encryption). These results demonstrate the expected trade-off between resource efficiency and performance.

The application-oriented evaluation further showed that both architectures are capable of supporting representative WSN packet sizes while maintaining deterministic execution latency suitable for resource-constrained sensing applications. Architecture 2 is particularly well suited to low-power sensor nodes where minimizing hardware resources and energy consumption is the primary design objective, whereas Architecture 3 is more appropriate for gateway nodes or higher-performance edge devices requiring increased data TP.

Overall, the results show that hardware-assisted Ascon offers an effective lightweight AEAD solution for secure WSN communication, balancing hardware cost, performance, and energy efficiency. The evaluation also provides practical guidance for selecting FPGA architectures according to WSN and IoT deployment requirements.

Limitations and Future Work

This study does not include complete WSN node implementation with an MCU, radio stack, and end-to-end communication protocol. Instead, we provide a system-level feasibility analysis based on synthesis-derived performance metrics. Future work will integrate the proposed accelerator into a full WSN platform (e.g., Contiki Next Generation (Contiki-NG) or RIOT Operating System (RIOT-OS)) to measure end-to-end latency, energy consumption, and protocol-level interactions.

The proposed Ascon accelerators are intended to complement existing WSN and IoT communication stacks. Future work will therefore focus on evaluating how the hardware architectures interact with complete protocol stacks such as Zigbee, 6LoWPAN, and Thread, where AES-CCM is traditionally employed [27].

Similarly, integration with higher-layer IoT protocols such as MQTT and CoAP, where cryptographic overhead must remain negligible compared to networking and broker delays [28], requires assessing the accelerator's behavior under realistic scheduling, buffering, and radio-interface constraints. Long-range systems such as LoRaWAN, where data rates are low but energy efficiency and predictability are critical, also represent promising targets for gateway-side acceleration of aggregated traffic [29]. Beyond classical WSNs, the low-latency characteristics of the proposed architectures suggest potential applicability to intra-vehicular sensor networks inspired by CAN-FD, where encryption latency must remain well below the typical 5 ms frame budget [30]. Validating these assumptions through full-stack prototypes and timing analysis forms a natural extension of this work.

The proposed hardware-assisted Ascon design extends beyond WSN/IoT use, with relevance to Industry 4.0/5.0 systems requiring secure low-latency communication [31] and cognitive-radio IoT networks needing lightweight, energy-efficient security under dynamic conditions [32]. Future work will integrate these architectures into such intelligent cyber-physical environments to assess performance under realistic workloads.

Although the architectures were evaluated on FPGA with application-oriented WSN analysis, a complete hardware-in-the-loop prototype integrating the MCU, FPGA accelerator, radio, and protocol stack remains outside the scope of this work. Consequently, end-to-end latency, interface overhead, packet delivery ratio, and total node energy consumption under realistic traffic have not been evaluated. Future work will validate these on integrated MCU–FPGA–radio platform under representative WSN conditions.

Ascon's cryptographic strength is established, but this work evaluates architecture and performance rather than implementation-level security. Physical attack resistance, including power, EM, timing, and fault-injection attacks, was not tested, nor were protocol-level behaviors such as replay protection or nonce-misuse effects, which depend on external communication-stack design. Future work will integrate countermeasures such as masking, hiding, fault detection, and secure nonce management into the FPGA architectures and assess their impact on resource use, frequency, power, latency, TP, and energy efficiency to determine practical security–cost trade-offs for constrained WSN platforms.

Acknowledgement: The authors would like to thank their respective institutions for providing the facilities, computational resources, and research environment that supported this research.

Funding Statement: This research is supported by the Korea Institute of Marine Science and Technology Promotion (KIMST), in 2022 through the Project is Development and Demonstration of Data Platform for AI Based Safe Fishing Vessel Design (Grant Number: RS-2022-KS221571).

Author Contributions: The authors confirm contribution to the paper as follows: conceptualization, Kuldashbay Avazov, Akmalbek Abdusalomov and Young Im Cho; methodology, Kuldashbay Avazov, Jasur Sevinov and Akmalbek Abdusalomov; software, Kuldashbay Avazov, Jasur Sevinov and Komil Tashev; validation, Kuldashbay Avazov, Jamila Arzieva, Tulkin Botirov and Alpamis Kutlimuratov; formal analysis, Kuldashbay Avazov, Akmalbek Abdusalomov and Boburjon Vafoev; investigation, Kuldashbay Avazov, Jasur Sevinov and Komil Tashev; resources, Young Im Cho and Akmalbek Abdusalomov; data curation, Kuldashbay Avazov, Jamila Arzieva and Tulkin Botirov; writing—original draft preparation, Kuldashbay Avazov; writing—review and editing, Jasur Sevinov, Akmalbek Abdusalomov, Boburjon Vafoev and Young Im Cho; visualization, Komil Tashev and Alpamis Kutlimuratov; supervision, Akmalbek Abdusalomov and Young Im Cho; project administration, Young Im Cho; funding acquisition, Young Im Cho. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: Data available on request from the authors. The data that support the findings of this study are available from the Corresponding Author, Young Im Cho, upon reasonable request.

Ethics Approval: Not applicable. This study did not involve human participants, animals, or identifiable personal data. Therefore, ethical approval and informed consent were not required.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Ojha A, Gupta B. Evolving landscape of wireless sensor networks: a survey of trends, timelines, and future perspectives. Discov Appl Sci. 2025;7(8):825. doi:10.1007/s42452-025-07070-6.
2. El Khediri S. Wireless sensor networks: a survey, categorization, main issues, and future orientations for clustering protocols. Computing. 2022;104(8):1775–837. doi:10.1007/s00607-022-01071-8.
3. Elsadig MA, Altigani A, Baraka MAA. Security issues and challenges on wireless sensor networks. Int J Adv Trends Comput Sci Eng. 2019;8(4):1551–9. doi:10.30534/ijatcse/2019/78842019.
4. Perrig A, Szewczyk R, Wen V, Culler D, Tygar JD. SPINS: security protocols for sensor networks. In: Proceedings of the 7th Annual International Conference on Mobile Computing and Networking; 2001 Jul 16–21; Rome, Italy. p. 189–99.
5. Boubiche DE, Athmani S, Boubiche S, Toral-Cruz H. Cybersecurity issues in wireless sensor networks: current challenges and solutions. Wirel Pers Commun. 2021;117(1):177–213. doi:10.1007/s11277-020-07213-5.
6. Feldhofer M, Dominikus S, Wolkerstorfer J. Strong authentication for RFID systems using the AES algorithm. In: Cryptographic Hardware and Embedded Systems—CHES 2004. Berlin/Heidelberg, Germany: Springer; 2004. p. 357–70.
7. Guşiţă B, Anton AA, Stângaciu CS, Stănescu D, Găină LI, Micea MV. Securing IoT edge: a survey on lightweight cryptography, anonymous routing and communication protocol enhancements. Int J Inf Secur. 2025;24(3):149. doi:10.1007/s10207-025-01071-7.
8. Sorescu TG, Chiriac VM, Stoica MA, Comsa CR, Soroaga IG, Contac A. Comparative performance analysis of lightweight cryptographic algorithms on resource-constrained IoT platforms. Sensors. 2025;25(18):5887. doi:10.3390/s25185887.
9. Sönmez Turan M, McKay K, Chang D, Bassham L, Kang J, Waller N, et al. Status report on the final round of the NIST lightweight cryptography standardization process. Gaithersburg, MD, USA: National Institute of Standards and Technology; 2023. Report No.: NIST IR 8454.
10. Jimale MA, Z'Aba MR, Kiah MLBM, Idris MYI, Jamil N, Mohamad MS, et al. Authenticated encryption schemes: a systematic review. IEEE Access. 2022;10:14739–66. doi:10.1109/access.2022.3147201.
11. Dobraunig C, Eichlseder M, Mendel F, Schläffer M. Ascon v1.2: lightweight authenticated encryption and hashing. J Cryptol. 2021;34(3):33. doi:10.1007/s00145-021-09398-9.
12. Ahmet M. High-performance FPGA implementations of lightweight ASCON-128 and ASCON-128a with enhanced throughput-to-area efficiency. In: Proceedings of the 2024 17th International Conference on Information Security and Cryptology (ISCTürkiye); 2024 Oct 16–17; Ankara, Turkiye. p. 1–7.
13. Khan S, Lee WK, Hwang SO. Scalable and efficient hardware architectures for authenticated encryption in IoT applications. IEEE Internet Things J. 2021;8(14):11260–75. doi:10.1109/JIOT.2021.3052184.
14. Khan S, Inayat K, Bin Muslim F, Ali Shah Y, Atif Ur Rehman M, Khalid A, et al. Securing the IoT ecosystem: ASIC-based hardware realization of Ascon lightweight cipher. Int J Inf Secur. 2024;23(6):3653–64. doi:10.1007/s10207-024-00904-1.
15. Karlof C, Sastry N, Wagner D. TinySec: a link layer security architecture for wireless sensor networks. In: Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems; 2004 Nov 3–5; Baltimore, MD, USA. p. 162–75.
16. Radhakrishnan I, Jadon S, Honnavalli PB. Efficiency and security evaluation of lightweight cryptographic algorithms for resource-constrained IoT devices. Sensors. 2024;24(12):4008. doi:10.3390/s24124008.

17. Widodo B, Fazrie M, Parulian D. Lightweight cryptography for IoT in wireless sensor networks: evaluating Speck, Simon, and Ascon using NS-3. Electron J Educ Soc Econ Technol. 2025;6(2):1161.
18. Artetxe E, Barambones O, Calvo I, Fernández-Bustamante P, Martin I, Uralde J. Wireless technologies for industry 4.0 applications. Energies. 2023;16(3):1349. doi:10.3390/en16031349.
19. Raptis T, Passarella A, Conti M. Performance analysis of latency-aware data management in industrial IoT networks. Sensors. 2018;18(8):2611. doi:10.3390/s18082611.
20. Sadeghi AR, Wachsmann C, Waidner M. Security and privacy challenges in industrial Internet of Things. In: Proceedings of the 52nd Annual Design Automation Conference; 2015 Jun 7–11; San Francisco, CA, USA. p. 1–6.
21. Manifavas C, Hatzivasilis G, Fysarakis K, Rantos K. Lightweight cryptography for embedded systems—a comparative analysis. In: Data privacy management and autonomous spontaneous security. Berlin/Heidelberg, Germany: Springer; 2014. p. 333–49.
22. Willig A. Recent and emerging topics in wireless industrial communications: a selection. IEEE Trans Ind Inform. 2008;4(2):102–24. doi:10.1109/TII.2008.923194.
23. Beg A, Al-Kharobi T, Al-Nasser A. Performance evaluation and review of lightweight cryptography in an Internet-of-things environment. In: Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS); 2019 May 1–3; Riyadh, Saudi Arabia. p. 1–6.
24. Curlin PS, Heiges J, Chan C, Lehman TS. A survey of hardware-based AES SBoxes: area, performance, and security. ACM Comput Surv. 2025;57(9):1–37. doi:10.1145/3724114.
25. Vucinic M, Selander G, Mattsson JP, Watteyne T. Lightweight authenticated key exchange with EDHOC. Computer. 2022;55(4):94–100. doi:10.1109/mc.2022.3144764.
26. Gross H, Wenger E, Dobraunig C, Ehrenhöfer C. Ascon hardware implementations and side-channel evaluation. Microprocess Microsyst. 2017;52:470–9. doi:10.1016/j.micpro.2016.10.006.
27. Qiu S, Cao R, Shi H, Li J, Li Y. 6WPSN: reliable and efficient IPv6 packet broadcast protocol for IEEE 802.15.4-based wireless powered sensor networks. Peer Peer Netw Appl. 2023;16(2):589–605. doi:10.1007/s12083-022-01421-5.
28. Seoane V, Garcia-Rubio C, Almenares F, Campo C. Performance evaluation of CoAP and MQTT with security support for IoT environments. Comput Netw. 2021;197(4):108338. doi:10.1016/j.comnet.2021.108338.
29. Centenaro M, Vangelista L, Zanella A, Zorzi M. Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios. IEEE Wirel Commun. 2016;23(5):60–7. doi:10.1109/MWC.2016.7721743.
30. Gruber B, Yordanov D, Mochel C. CAN FD: the easy path to faster communication speed. Warrendale, PA, USA: SAE International; 2018.
31. Nagy M, Valaskova K, Lazaroiu G. Digitalization-based predictive maintenance systems, Internet of Things sensor networks, and machine intelligence algorithms for industry 4.0/5.0 manufacturing processes. Systems. 2026;14(3):281. doi:10.3390/systems14030281.
32. Fernando X, Lăzăroiu G. Spectrum sensing, clustering algorithms, and energy-harvesting technology for cognitive-radio-based Internet-of-things networks. Sensors. 2023;23(18):7792. doi:10.3390/s23187792.