Benchmarking Lightweight Cryptography: ASCON-128 vs. AES-128-GCM for IoT Environments*

*Note: Sub-titles are not captured for https://ieeexplore.ieee.org and should not be used

1st Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

2nd Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

3rd Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

***Abstract*—This paper presents a comparative analysis of ASCON-128 (NIST LWC Standard) and AES-128-GCM on resource-constrained environments. We focus on CPU latency, memory usage, and code overhead.**

***Index Terms*—Lightweight Cryptography, ASCON, AES-GCM, IoT Security, Benchmarking**

I. Introduction

The Internet of Things (IoT) has rapidly expanded...

A. Problem Statement

Standard cryptographic algorithms like AES-GCM can be computationally expensive for 8-bit or 16-bit microcontrollers [1].

B. Contribution

This paper provides:

- A deterministic benchmark of ASCON-128 vs AES-128-GCM.
- Memory usage analysis using `tracemalloc`.
- Latency comparison across varying payload sizes.

II. Background

A. AES-128-GCM

Advanced Encryption Standard (AES) in Galois/Counter Mode (GCM) is the current industry standard for high-performance Authenticated Encryption with Associated Data (AEAD)...

B. ASCON-128

ASCON was selected by NIST as the standard for lightweight cryptography in 2023. It is a sponge-based cipher designed for...

Identify applicable funding agency here. If none, delete this.

III. Methodology

A. Experimental Setup

We utilized Python 3.10 implementations for both algorithms.

- **Hardware**: [Insert CPU Info]
- **Libraries**: `pycryptodome` (AES) and `ascon` (native).

B. Metrics

We measured:

1) **Encryption Latency**: Time taken for encryption operations.
2) **Memory Overhead**: Peak RAM usage during crypto operations.
3) **Throughput**: Bytes processed per second.

IV. Results and Analysis

A. Latency Analysis

Figure **??** shows the encryption time for varying payload sizes...

B. Memory Usage

ASCON demonstrated lower peak memory usage compared to AES-GCM...

V. Conclusion

In conclusion, ASCON-128 proves to be a viable alternative to AES-GCM for constrained devices, offering significant memory savings...

References

[1] NIST, "Lightweight cryptography," https://csrc.nist.gov/Projects/lightweight-cryptography, 2023, accessed: 2025-12-20.