Chapter 2
Metaverse Security: Performance Evaluation of Cryptography Techniques

Indranil Saha
http://orcid.org/0009-0003-9802-7630
NIIT University, India

Anuva Aggarwal
http://orcid.org/0009-0006-3949-0889
NIIT University, India

Taher Aurangabadi
http://orcid.org/0009-0008-3127-5943
NIIT University, India

Zeesha Mishra
http://orcid.org/0009-0003-9802-7630
NIIT University, India

ABSTRACT

Encryption standards have been necessitated by these things, which include border security, defense intelligence, and distributed systems of the IoT. This paper has compared the performance of AES-256 and ASCON-128 in terms of performance based on intensive experimental data on seven cryptographic measures at four standardized payload sizes. The findings reveal that AES-256 always achieves high throughput, low encryption latency, and a reduced number of CPU cycles per byte. These properties make AES-256 very well adapted to bandwidth-intensive and latency-critical applications. Conversely, ASCON-128 has slower performance in the tested implementations, but has more predictable execution characteristics. On the whole, the outcome is an indication of an obvious application-specific trade-off:

DOI: 10.4018/979-8-2600-2313-6.ch002

AES-256 is more appropriate for the high-performance communication system. In comparison to the ASCON-128, which is better suited to the memory-limited and low-power IoT environment, where in-built authentication and deterministic behavior are more important than raw speed.

INTRODUCTION TO MODERN ENCRYPTION STANDARDS

The concept of secure communication is considered to be one of the main demands of modern digital systems. Due to the growing importance of both the use and support of heterogeneous settings in Internet of Things (IoT) nodes at extreme limits, high-bandwidth surveillance infrastructures at extreme limits. In data transmission, the choice and optimization of cryptographic primitives have become a major design factor. This has necessitated a change in the way encryption algorithms are tested and analysed, not only in terms of their theoretical security properties but also in a performance sense with respect to aspects like latency time, throughput, cost of computation, memory size, and scalability to deployment issues Shannon, 1948). Due to its efficiency and scalability, symmetric-key cryptography remains to be considered the solution of choice in today's real-time applications to provide privacy and integrity of data (Hallem et al., 2025). Nevertheless, the high-speed diversification of application environments has been exposed as constraints inherent in traditional cryptographic standards when utilized on the resource-constrained platforms. This has led to low-power cryptographic algorithms and low-memory algorithms, as well as high-performance encryption methods that are used in throughput-intensive applications. The knowledge of such opposing design philosophies is then deemed critical to the choice of the right encryption standards in the contemporary security systems (Daemen & Rijmen, 2002; Hassan, 2020).

This chapter explores the inherent differences between lightweight and high-throughput design methods in cryptography by describing a thorough, performance-based comparison between two standard encryption algorithms representing performance-sensitive cryptography design: ASCON-128, an authenticated encryption algorithm standardized within the National Institute of Standards and Technology's Lightweight Cryptography project, and AES-256, a common high-performance block cipher. Before the experimental results and optimization techniques are presented, the contextual reasons and the cryptographic underlying basis that justify this comparison are initially laid out (Meltem et al., 2025; Al-Zubaidie, 2026a).