Chapter 4
A Software-Based ASCON-QPP Security for Lightweight Metaverse Applications

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

Dhruvika Bansal
http://orcid.org/0009-0000-5825-6410
NIIT University, India

Garvit Bajaj
http://orcid.org/0009-0003-4331-8019
NIIT University, India

ABSTRACT

The growing dependence on data-centric software systems demands strong protection of sensitive information, where confidentiality, integrity, and high-quality randomness are critical. Permutation-based cryptography provides structured diffusion and unpredictability for secure software environments. ASCON, selected by National Institute of Standards and Technology (NIST) as a lightweight cryptography standard, offers an efficient and modular permutation suitable for experimentation. The Quantum Permutation Pad (QPP) introduces highly nonlinear, entropy-rich byte-level permutations to enhance state mixing. This chapter integrates ASCON with QPP in software across baseline, 6-round, and 12-round configurations and evaluates performance using randomness tests, bit-distribution, avalanche effect,

DOI: 10.4018/979-8-2600-2313-6.ch004

and key sensitivity. Results show avalanche improvements of 21.7% and 39.1%, a 0.25% entropy increase, 100% serial correlation reduction, ~4% bit-bias reduction, and only 1–1.5% throughput overhead.

INTRODUCTION

Large amounts of sensitive data are handled by contemporary software systems across cloud services, communication platforms, embedded devices, and sensor networks, which raises the demand for dependable and mathematically sound cryptographic techniques. Permutation-based cryptography has become a strong candidate in this context because it provides diffusion, randomness, and sensitivity to input changes within lightweight and software-driven designs, which are especially valuable for resource-constrained and high-throughput environments (Mishra & Acharya, 2023; Raja et al., 2023). Because of its clean, round structure and well-separated substitution, diffusion, and constant-injection operations, ASCON—which was chosen for the NIST Lightweight Cryptography process—is particularly noteworthy and appropriate for controlled experimental modification (Turan et al., 2024; Jana, 2024).

In addition to traditional embedded and cloud platforms, new virtual ecosystems, such as the metaverse, raise security problems because of the ongoing interaction in real time, high data rates, and rigid latency requirements (Tahayur, 2025). Lightweight and efficient cryptographic primitives are needed in these environments to secure users, virtual assets, and state synchronisation of distributed platforms. The symmetric permutation-based encryption systems have low computational costs and are appropriate for the encryption of communication pipelines in the metaverse. This also represents a segment of the next generation of virtual and immersive applications where ASCON-QPP is a viable security primitive to be explored and studied.

Figure 1. The function of lightweight symmetric encryption and a high-level metaverse security architecture.