Paper Review: Optimized High-Performance Lightweight Cryptography Combining Hyperchaos,Reversible Elementary Cellular Automata, and DNA Computing: Efficient Implementation on Zynq SoC

isomo

May 23, 2025

1 Quick Look at the Paper

1.1 Abstract

- To address these challenges, this paper presents an optimized high-performance lightweight cryptosystem leveraging **hyperchaos,reversible elementary cellular automata (R-ECA), and DNA computing**, implemented on an SoC-FPGA platform.
- The proposed cryptosystem employs a single-round block cipher algorithm integrating four key processes: permutation, DNA encoding, R-ECA transformation, and a whitening operation. The Lorenz hyperchaotic system is utilized for secure key generation, ensuring high sensitivity and robustness.

Note

this paper is combined the much techniques, not claim the motivation of the hyperchaos, reversible elementary cellular automata, and DNA computing on the Abstract.

1.2 Introduction

Note

- The related works comparison with the motivation for using hyperchaos, reversible elementary cellular automata, and DNA computing is not sufficient.
- The paper too much engineering, only focus on how to do, not focus on why to do.
- The typesetting is not compact, the table is too large, and the figures are not clear.

So here we do not detail reading the paper.

2 Issues

- Lack of clear motivation for combining hyperchaos, reversible elementary cellular automata (R-ECA), and DNA computing.
- Insufficient comparison with related works, especially regarding the rationale for using the chosen techniques.
- The paper is overly focused on engineering implementation (how), with little discussion on the underlying reasons (why) for the design choices.
- Typesetting issues: the layout is not compact, tables are too large, and figures lack clarity.

3 Comments

The manuscript "Optimized High-Performance Lightweight Cryptography Combining Hyperchaos, Reversible Elementary Cellular Automata, and DNA Computing: Efficient Implementation on Zynq SoC." proposes a hardware-oriented cryptosystem. While the hardware implementation demonstrates some engineering merit, the cryptographic design lacks sufficient justification and rigorous analysis. The manuscript also exhibits significant presentation and formatting issues. Addressing these scientific concerns would require a complete redesign and a comprehensive, standards-compliant security evaluation. Therefore, rejection is recommended in its current form. The following points summarize the main issues:

- **Single-round design is insecure.** Modern lightweight block ciphers require 10–32 rounds for proper diffusion, but the proposed scheme uses only one round without formal justification or cryptanalysis.
- **Security evaluation is limited to image-statistical tests.** The manuscript reports only NPCR, UACI, histogram, and NIST randomness results, with no standard cryptanalytic evaluation (differential, linear, algebraic, or advanced attacks).
- **Key-space calculation is incorrect and exaggerated.** The calculation multiplies incompatible bases and overstates the effective key space.
- **Performance claims are inconsistent and unverifiable.** Throughput and timing data do not match, and power consumption is reported without a clear measurement methodology.
- **No threat or attacker model is defined.** The manuscript does not specify which attacks the design is intended to resist.
- **Confusion between image encryption and block cipher.** The evaluation is conducted only on images, yet the work claims to propose a generic lightweight cipher.
- **Unclear design rationale.** The manuscript does not justify the use of hyperchaos, R-ECA, and DNA computing instead of standard lightweight ciphers.
- **Presentation and formatting problems.** Figures are low-resolution, tables are not normalized, and reference formatting is inconsistent.