Manuscript number**: TCAS-I-01399-2025**

Title**:** **Energy-efficient high-throughput encryption block using a discrete-space chaotic map and an AxRMU multiplier**

**The paper proposes an energy-efficient, high-throughput chaotic cipher using a discrete-space chaotic map with an approximate Radix-4 multiplier (AxRMU), presents interesting results showing energy reductions compared to conventional ciphers (76% vs. chaotic ciphers, 74% vs. AES, 7% vs. Ascon). While the combination of chaotic cryptography with approximate computing is novel and shows promising energy efficiency improvements, several significant issues need to be addressed for *major revision*. The security analysis requires strengthening, implementation details need clarification, and the throughput evaluation methodology needs improvement.**

1. Throughput Evaluation Methodology: The throughput calculations appear to be based on a specific operating frequency rather than the maximum achievable frequency. For a fair comparison and to demonstrate true high-throughput capability, the authors must provide maximum frequency data and recalculate throughput metrics accordingly. This is critical for validating the high-throughput claims.
2. Mode of Operation Inconsistency: The paper claims high-throughput operation but uses Cipher Block Chaining (CBC) mode for image encryption, which inherently limits parallelization. For true high-throughput applications, Counter (CTR) mode would be more appropriate. The comparison should include CTR-mode compatible ciphers or justify the CBC choice.
3. Energy-Efficiency vs. High-Throughput Trade-off: The paper claims both energy efficiency and high throughput, but these goals can be conflicting. A more detailed analysis of how the approximate multiplier achieves both simultaneously would strengthen the contribution.
4. Security Against Quantum Attacks: Given that each chaotic map operates on 32-bit values, the paper lacks discussion of quantum security. With quantum computing advancement, 32-bit key spaces may be vulnerable to quantum attacks. The authors should address quantum resistance or acknowledge this limitation.
5. Power Analysis Attack Resistance: The ASIC implementation results lack discussion of side-channel attack resistance, particularly power analysis attacks. Given the approximate computing approach, power consumption patterns might leak information about the encryption process.