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

NOTE: the Energy-efficient & high-throughput can both get?

Quick reading the manuscript

Abstract

- This work proposes a high-throughput, energy-efficient chaotic cipher that employs a **discrete-space chaotic map** as the pseudo-random number generator (PRNG). The most complex operation in the map is an integer multiplication, implemented using an **Approximate Radix-4 multiplier** (AxRMU) to leverage approximate computing.
- The results of the ASIC synthesis show that the use of the approximate multiplier leads to reductions of 5% in power, energy, and area compared to the exact Radix multiplier. Furthermore, the proposed cipher achieves a 76% reduction in energy consumption (pJ/bit) compared to the state-of-the-art chaotic cipher using the *AxRMU multiplier*, a 74% reduction compared to *AES*, and a 7% reduction relative to the loop-folder implementation of the *Ascon*.
- Security evaluations confirm that the cipher is resistant against statistical, differential, brute-force, and chosen-plaintext attacks.

NOTE: use the block cipher to encrypt the image is suitable. if the block size is lower than the image size, the image information will be public. The same part of the image will be same in the encrypted image. **IF we use the *CTR-MODE* this case will not happen.** Here the throughput is on the specific frequency, but for the most throughput, need use the *Max frequency* to calculated the throughput, so please add the *Max frequency* data.

Multipliers

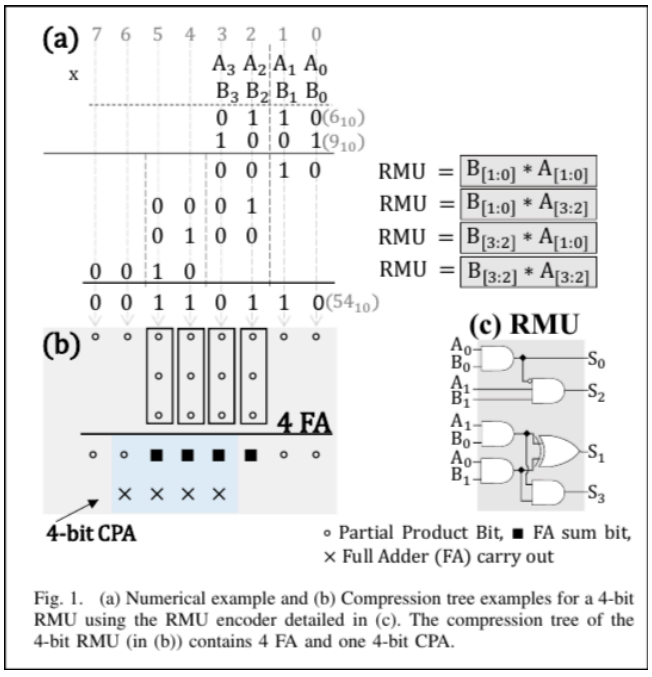

Fig. 1. (a) Numerical example and (b) Compression tree examples for a 4-bit RMU using the RMU encoder detailed in (c). The compression tree of the 4-bit RMU (in (b)) contains 4 FA and one 4-bit CPA.

Abbildung 1: Radix-4 multiplier unit (RMU)

NOTE: The Abbildung 1 is split the big space to small space, then to parallel the multiplication, finally to reduce the latency. The *AxRMU* use the approximate computing to reduce the power and energy consumption, from seven to four gates on the *AxRMU-4* multiplier.

discrete-space chaotic map
The discrete-space chaotic map is defined by the following equations:

$$x(i) = s \oplus x(i-1) \oplus x(i-2)$$

$$s = (z \ll (z\%32)) \mid (z \gg (32 - z\%32))$$

$$z = \left(\frac{x(i-1)}{16} + 1\right) \times ((x(i-1) \bmod 2^{16} + 1) + 1)$$

where $\oplus$ denotes the XOR operation, $\ll$ and $\gg$ are left and right bit shift operations respectively, and $\mid$ represents the bitwise OR operation.

Image encryption algorithm
NOTE: here each chaotic map is a 32-bit, if use the quantum computing to attacks the chaotic map is security?

NOTE: the image encryption use the Cipher Block Chaining mode, but the high-throughput is use the Count mode CTR. So if talked the encryption is high-throughput need to compared with the CTR mode, which supported the CTR mode cipher.

Security
ISSUE: the Table III & Table II occupied order is inverse.

ASIC implementation & results
ISSUE: it can to resistant the power analysis attack?

Review Comments

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.

Detailed Comments

- **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.
- **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.
- **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.
- **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.
- **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.