PARALLEL ALGORITHMS IN ENCRYPTION PROBLEMS

Dinara BUCILA,

masterandă, anul II, Program: SMMSPA, Facultatea de Matematică și Informatică, Universitatea de Stat din Moldova

CZU: 004.032.24:004.42 E-mail:bucila.dinara@usm.md

Escaladarea rapidă a atacurilor cibernetice la nivel global, reflectată prin depășirea pragului de 5,5 miliarde de conturi compromise în anul 2024, subliniază necesitatea stringentă a unor soluții de protecție a datelor care să combine scalabilitatea, robustețea și eficiența operațională. Prezenta lucrare propune o implementare paralelă a algoritmului Advanced Encryption Standard (AES), optimizată pentru execuție pe un cluster de calcul de înaltă performanță (HPC), prin utilizarea interfeței Message Passing Interface (MPI). Scopul urmărit constă în convertirea procesului secvențial de criptare a fișierelor de mari dimensiuni într-o soluție paralelă, performantă și extensibilă. Valorificând paralelizarea la nivel de date și structura matematică riguroasă a AES, fundamentată pe câmpurile Galois, implementarea demonstrează o armonizare între consistența teoretică și eficiența practică în criptarea securizată a volumelor masive de informații.

Introduction

According to recent cybersecurity reports [1], the number of compromised accounts has increased almost eightfold from 730 million in 2023 to over 5.5 billion in 2024 — the equivalent of 180 accounts being compromised every second. The average cost of a data breach is now over 4.88 million USD, and companies may face regulatory fines of up to 4% of their global annual turnover due to insufficient data protection.

Sequential encryption methods struggle to meet the demands of modern data scales. To overcome this, the research proposes a parallel software implementation of AES, executed on the HPC cluster at Moldova State University. The use of parallel computing not only accelerates encryption but also ensures that the process remains stable and functional even under adverse conditions — a key characteristic of a robust system.

Motivation for Integrating AES with Parallel High-Performance Architectures

Advanced Encryption Standard is the global symmetric encryption standard widely adopted in governmental, financial, and industrial domains. It is built on strong algebraic foundations and has withstood over two decades of scrutiny without any practical vulnerabilities. No known real-world attack has successfully broken AES, and its mathematical structure makes it highly resilient to cryptanalysis.

High-Performance Computing clusters provide the ideal infrastructure to scale encryption efforts. By adding more processing nodes, the system can handle increasingly large files in parallel, significantly reducing execution time.

Mathematical Structure of AES

The Advanced Encryption Standard operates over the finite field GF(2^8), where each byte (0–255) is represented as a polynomial of degree ≤ 7 with coefficients in GF(2). Among its core operations is SubBytes, which performs a non-linear byte substitution through multiplicative inversion in the finite field GF(2^8), followed by an affine transformation. This is complemented by ShiftRows, a transposition step that cyclically shifts the rows of the state matrix, thereby contributing to diffusion. The MixColumns operation further enhances diffusion by applying a linear transformation to each column of the state matrix, effectively mixing the byte values. Finally, AddRoundKey integrates the cipher key into the encryption process by executing a bitwise XOR between the current state and a round-specific portion of the key.

As an example, the byte 0x53 is transformed by finding its multiplicative inverse in GF(2^8), which is 0xCA (since 0x53 × 0xCA ≡ 1 mod 0x11B). Such operations provide strong confusion and diffusion, the pillars of cryptographic security.

Parallel Implementation Using MPI

The AES encryption process is parallelized using a data-level strategy. The input file — for example, a password database — is divided into segments that are independently encrypted by separate MPI processes. The implementation steps include MPI Initialization, input file loading, distributing lines to processes, encrypting each segment independently, writing results to output file and finalizing MPI execution.

This method takes advantage of AES’s block-oriented structure: no synchronization between processes is needed since each data block can be encrypted autonomously. It ensures minimal communication overhead and near-linear scalability.

Results and Practical Value

The proposed implementation successfully transforms slow, sequential encryption into a parallel, scalable system capable of handling large datasets efficiently (Figure 5.1).

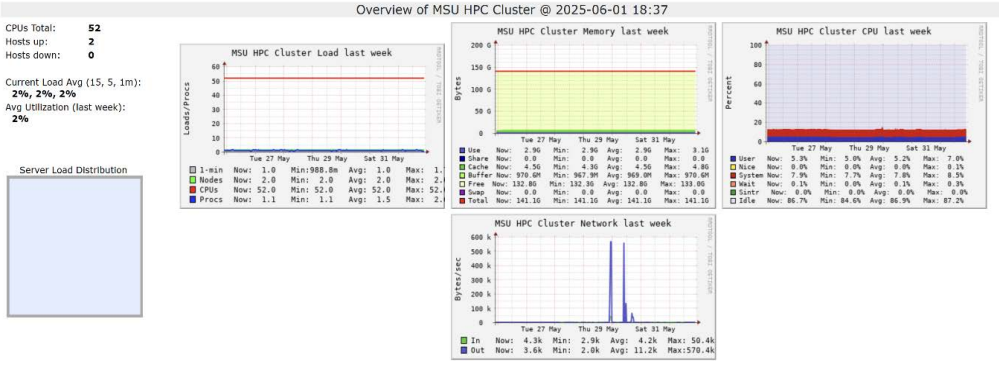


Figure 5.1 AES parallel execution results

Conclusion

The research demonstrates that the Advanced Encryption Standard can be effectively parallelized for high-performance environments using MPI. The resulting system achieves robust, scalable, and fast encryption — characteristics essential in the current cybersecurity climate. By aligning mathematical security with computing efficiency, the solution meets both theoretical and practical demands, making it suitable for a wide range of real-world applications.

References:

1. Cost of a Data Breach Report 2024. IBM [accessed: 10 march 2025]. Available: https://www.ibm.com/reports/data-breach

Recommended
***Boris HÎNCU**, conf. univ., doctor.*