Faculty of Computers
& Artificial Intelligence

Benha University

InTouch

A senior project submitted in partial fulfillment of the requirements for the degree of Bachelor of Computers and Artificial Intelligence.

Scientific Computing Departement

Project Team

1. Mohamed Ahmed Elsayed Emary
2. Abdelfattah Zakaria Abdelfattah Morsy
3. Mohamed Abdelfattah Ahmed Abdelfattah
4. Dalia Abdullah Mohamed Mahmoud
5. Shrouk Elsayed Mohamed Abdelmoem
6. Sara Reda Abdallah Elshiekh

Under Supervision of

Dr. Sayed Badr

Benha, February 2024

F B R R U A R Y – 2 0 2 4

Acknowledgement

We would like to express our sincere gratitude to our project supervisor, Dr. Sayed Badr, for his invaluable guidance and support throughout the completion of our graduation project. His expertise and insightful feedback were instrumental in shaping our research and refining our approach. We are particularly grateful for his willingness to offer constructive criticism, which challenged us to think critically and improve the quality of our work.

Declaration

We hereby certify that this material, which we now submit for assessment on the program of study leading to the award of Bachelor of Computers and Artificial Intelligencein (High-Speed Encryption Algorithm with Polynomial Roots) is entirely our own work, that we have exercised reasonable care to ensure that the work is original, and does not to the best of our knowledge breach any law of copyright, and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of ourwork.

Signed: _____

Signed: _____

Signed: _____

Signed: _____

Signed: _____

Signed: _____

February 10, 2024

Abstract

Encryption algorithms play a critical role in protecting sensitive data in the digital age. However, traditional symmetric encryption methods like AES suffer from high computational complexity that hinders performance. Our project proposes a novel polynomial interpolation based encryption algorithm that aims to accelerate encryption and decryption speeds. The algorithm leverages polynomials generated from secret keys. It then uses an efficient hybrid root finding technique called HybridBF to encode messages into ciphertext roots and decode them back to plaintext. Extensive testing on 1000 sample plaintext-key pairs shows the new algorithm is significantly faster than AES for both encryption and decryption. The hybrid root finder combines aspects of bisection and false position methods, demonstrating faster convergence than either individual technique. By exploiting polynomials and highly optimized root finding, this project delivers an encryption algorithm with superior efficiency while maintaining security. The improved performance could enable broader adoption of strong encryption across communication networks and data storage systems.